Benutzerhandbuch

McAfee Security-as-a-Service-Erweiterung -

Zur Verwendung mit ePolicy Orchestrator® 4.6.0-Software

COPYRIGHT
Copyright © 2011 McAfee, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übermittelt, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN
AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung
HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einleitung **5**

Informationen zu diesem Handbuch 5

Zielgruppe 5

Konventionen 5

Quellen für Produktinformationen 6

1 Einführung in die Security-as-a-Service-Erweiterung **7**

Verwaltung von McAfee SaaS-Schutzdiensten 7

Erforderliche Komponenten 8

Einrichtung und Integration von Komponenten 8

2 Installieren und Konfigurieren der Erweiterung **11**

Übersicht über Installation und Setup 11

Funktionen, die der ePolicy Orchestrator-Umgebung hinzugefügt wurden 12

Übersicht über die Funktionskonfiguration 13

Installieren der Produkterweiterung 14

Konfiguration registrierter Server 16

Registrieren eines SecurityCenter-Kontos 17

Anzeigen oder Bearbeiten einer Liste mit registrierten SecurityCenter-Konten 18

Löschen eines registrierten SecurityCenter-Kontos 19

Datensynchronisierung mit SecurityCenter 19

Informationen zu den synchronisierten Daten 20

Erstellen eines Synchronisierungspunkts in der Systemstruktur 21

Synchronisieren von Daten vom SecurityCenter 22

Anzeigen des Status von Synchronisierungspunkten 25

Konfiguration von Berechtigungssätzen 26

Konfigurieren von Berechtigungssätzen für Benutzerrollen 27

Konfigurieren eines Synchronisierungsadministrator-Kontos 27

Erstellen oder Aktualisieren eines Synchronisierungsadministrator-Kontos 28

3 Überwachen und Verwalten der McAfee SaaS-Sicherheit **29**

Übersicht über den Überwachungsprozess 29

Funktionen zur Überwachung von Schutzdiensten 30

Dashboards und Monitore für Security-as-a-Service 31

Abfragen und Berichte für Security-as-a-Service 33

Vordefinierte Abfragen 33

Benutzerdefinierte Abfragen und Berichte 33

Systeminformationsseite 34

Bedrohungsereignisprotokoll 35

Bereinigen von Bedrohungsereignissen 35

Öffnen von SecurityCenter 36

Kompatibilität mit anderen McAfee-Produkten 36

Überlegungen zur Verwendung von McAfee Risk Advisor 36

4 Fehlerbehebung **41**
Lösungen zur Fehlerbehebung 41
Manuelle Löschung von Dateien und Ereignissen 45
Manuelles Löschen von Daten 45
Weitere Informationen 46

Index **49**

Einleitung

Dieses Handbuch enthält die Informationen, die Sie in den einzelnen Phasen der Produktnutzung benötigen – von der Installation über die Konfiguration bis hin zur Fehlersuche.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel oder *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; Einführung eines neuen Begriffs; Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe` oder `Pfad`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; der Pfad eines Verzeichnisses oder Programms.
`Code`	Ein Code-Beispiel.
Benutzeroberfläche	Wörter aus der Benutzeroberfläche, einschließlich Optionen, Menüs, Schaltflächen und Dialogfeldern.
Hypertext-Blau	Ein funktionsfähiger Link auf ein Thema oder eine Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.

Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.

Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

McAfee stellt Ihnen die Informationen zur Verfügung, die Sie in den einzelnen Phasen der Produktimplementierung benötigen – von der Installation bis hin zur täglichen Nutzung und Fehlerbehebung. Nach der Produktveröffentlichung erhalten Sie Informationen zu diesem Produkt online in der KnowledgeBase von McAfee.

Vorgehensweise

1 Wechseln Sie zum McAfee Technical Support ServicePortal unter http://mysupport.mcafee.com.

2 Greifen Sie unter **Self Service** (Online-Support) auf den erforderlichen Informationstyp zu:

Zugriff auf	Vorgehensweise
Benutzerdokumentation	1 Klicken Sie auf **Product Documentation** (Produktdokumentation). 2 Wählen Sie ein Produkt und dann eine Version aus. 3 Wählen Sie ein Produktdokument aus.
KnowledgeBase	• Klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen), um Antworten auf Ihre produktbezogenen Fragen zu erhalten. • Klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchblättern), um Artikel nach Produkt und Version aufzulisten.

1 Einführung in die Security-as-a-Service-Erweiterung

Mit der McAfee® Security-as-a-Service-Berichtserweiterung können Sie den Status von Computern überwachen, die mit McAfee Security-as-a-Service (McAfee SaaS)-Diensten geschützt und auf der McAfee® SecurityCenter-Website verwaltet werden.

Die Erweiterung ist für eine Nutzung mit McAfee® ePolicy Orchestrator (McAfee ePO™)-Software der Version 4.6 oder später vorgesehen.

Inhalt

- *Verwaltung von McAfee SaaS-Schutzdiensten*
- *Erforderliche Komponenten*
- *Einrichtung und Integration von Komponenten*

Verwaltung von McAfee SaaS-Schutzdiensten

Mit der Security-as-a-Service-Berichtserweiterung können Sie mit der ePolicy Orchestrator-Konsole Status- und Ereignisinformationen verwalteter Systeme überwachen, die durch McAfee SaaS-Dienste geschützt werden.

Ihr Abonnement für McAfee SaaS-Schutzdienste umfasst ein Konto für das webbasierte Verwaltungstool SecurityCenter, das Folgendes enthält:

- **Datenbank-Server**: Enthält Informationen über die McAfee SaaS-Schutzdienste und die damit geschützten Computer.
- **SecurityCenter-Konsole**: Zeigt Informationen aus der Datenbank, um die Systeme, in denen McAfee SaaS-Dienste installiert sind, zu verwalten (z. B. durch Erstellen von Richtlinien und ausführlichen Entdeckungsberichten).

Die Erweiterung ermöglicht eine Kommunikation zwischen dem ePolicy Orchestrator-Server und einem oder mehreren SecurityCenter-Konten. Anschließend werden Daten (oder Kopien) aus der Datenbank von SecurityCenterabgerufen und mit der Datenbank von ePolicy Orchestrator synchronisiert. Mithilfe der Überwachungs- und Berichtsfunktionen der Erweiterung können Sie grundlegende SaaS-Informationen in derePolicy Orchestrator-Konsole anzeigen.

Erforderliche Komponenten

Zur Verwaltung der McAfee SaaS-Schutzdienste mit der Security-as-a-Service-Erweiterung müssen die folgenden Komponenten eingerichtet und ausgeführt werden.

- **Server und Datenbank von ePolicy Orchestrator 4.6 (oder höher)**: Das Verwaltungstool für Unternehmenssicherheit, mit dem Aktivitäten überwacht und Berichte zu verwalteten Systemen erstellt werden, auf denen Sicherheitsprodukte von McAfee ausgeführt werden.
- **McAfee SecurityCenter** : Ein webbasiertes Verwaltungstool für McAfee SaaS-Dienste. Es wird von Site-Administratoren verwendet, um Client-Software zu installieren, Richtlinien auszubringen, Aktivitäten und Entdeckungen zu überwachen, Berichte zu erstellen und Kontoinformationen zu verwalten.
- **Security-as-a-Service-Erweiterung**: Software zur Bereitstellung einer Schnittstelle zwischen SecurityCenter und dem Server und der Datenbank von ePolicy Orchestrator.
- **McAfee SaaS-Schutzdienste**: Schutzdienste, mit denen auf Client-Computern Aktivitäten überwacht und Berichte dazu erstellt sowie Bedrohungen entdeckt und Reaktionsmaßnahmen ergriffen werden. Einige Schutzdienste umfassen auch die Konfiguration von Konten oder die Installation von Client-Softwarekomponenten.

Einrichtung und Integration von Komponenten

Sobald Ihre ePolicy Orchestrator-Umgebung ausgeführt wird, müssen vier Schritte durchgeführt werden, um eine ordnungsgemäße Interaktion zwischen den Verwaltungskomponenten und den McAfee SaaS-Schutzdiensten zu gewährleisten.

Wenn Sie bereits ein SecurityCenter-Administratorkonto eingerichtet und alle erforderlichen Installationen, Aktivierungen oder Konfigurationen für McAfee SaaS-Schutzdienste vorgenommen haben, beginnen Sie mit Schritt 3.

Prozessübersicht

1: Richten Sie in SecurityCenter ein Administratorkonto ein.

Beim Kauf eines Abonnements vonMcAfee SaaS-Diensten veranlasstMcAfee oder Ihr Dienstanbieter Folgendes:

- Es wird ein Konto für Sie erstellt.
- Es wird ein webbasiertes Verwaltungstool (SecurityCenter) für Sie eingerichtet. Mit SecurityCenter wird der Status der durch Ihre McAfee SaaS-Dienste geschützten Computer verwaltet.
- Ihnen werden die Informationen zur Anmeldung bei der SecurityCenter-Konsole gesendet. Sie müssen sich bei Ihrem Konto anmelden und bei Bedarf Einstellungen konfigurieren.

2: Installieren Sie die Client-Software, und aktivieren Sie die gewünschten Schutzdienste.

Bei einigen Schutzdiensten ist eine Installation von Software auf Client-Computern, eine Aktivierung oder Konfiguration erforderlich, bevor der Schutz wirksam wird. Weitere Informationen enthält die Begrüßungs-E-Mail, die Sie bei Abonnierung der McAfee SaaS-Dienste erhalten haben, sowie die in der SecurityCenter-Konsole auf der Seite **Hilfe und Support** erhältliche Dokumentation.

Überprüfen Sie, bevor Sie fortfahren, ob in der SecurityCenter-Konsole Daten zu den mit McAfee SaaS verwalteten Systemen angezeigt werden. Sehen Sie beispielsweise auf der Seite **Computer** nach, um sicherzustellen, dass die verwalteten Systeme im Konto angezeigt werden. Zeigen Sie die Widgets auf der Seite **Dashboard** an, um Status- und Entdeckungsinformationen auf einen Blick zu sehen. In der ePolicy Orchestrator-Konsole können Informationen jedoch erst angezeigt werden, wenn sie in SecurityCenter verfügbar ist.

3: Installieren Sie die Erweiterung, und richten Sie sie ein.

Anweisungen finden Sie in diesem Handbuch und in einer Kurzanleitung in der SecurityCenter-Konsole auf der Seite **Dienstprogramme** auf der Registerkarte **ePO-Server**.

4: Verwalten Sie Ihre mit McAfee SaaS-Diensten geschützten Computer von zwei Standorten aus.

Nach Abschluss der Installation können Sie auf zwei Konsolen Informationen zu verwalteten Systemen einsehen:

- Die **ePolicy Orchestrator-Konsole** überwacht Status- und Ereignisinformationen. Installieren Sie Client-Software, konfigurieren Sie Richtlinien, oder erledigen Sie andere Verwaltungsaufgaben durch Auswahl der Links im **McAfee SecurityCenter**-Monitor im **Security-as-a-Service**-Dashboard, um die SecurityCenter-Konsole zu öffnen.
- Die **SecurityCenter-Konsole** dient zur Erstellung benutzerdefinierter Richtlinien, zur Installation von Client-Software und zur Ausführung ausführlicher Berichte. Weitere Informationen finden Sie in der Dokumentation zu McAfee® SaaS Endpoint Protection. Diese befindet sich in der SecurityCenter-Konsole auf der Seite **Hilfe und Support**.

2 Installieren und Konfigurieren der Erweiterung

In diesen Abschnitten werden Installation, Einrichtung und Konfiguration der Erweiterungsfunktionen erläutert.

Inhalt

- *Übersicht über Installation und Setup*
- *Funktionen, die der ePolicy Orchestrator-Umgebung hinzugefügt wurden*
- *Installieren der Produkterweiterung*
- *Konfiguration registrierter Server*
- *Datensynchronisierung mit SecurityCenter*
- *Konfiguration von Berechtigungssätzen*
- *Konfigurieren eines Synchronisierungsadministrator-Kontos*

Übersicht über Installation und Setup

Installation und Einrichtung der Erweiterung erfolgen in vier allgemeinen Schritten.

Prozessübersicht

1 **Laden Sie die Erweiterung herunter, und installieren Sie sie.**

Laden Sie die .ZIP-Datei für die Produkterweiterung entweder von der SecurityCenter- oder der ePolicy Orchestrator-Konsole herunter, und installieren Sie anschließend die Erweiterung über die ePolicy Orchestrator-Konsole.

2 **Registrieren Sie Ihr SecurityCenter-Konto mit der ePolicy Orchestrator-Software.**

Hierfür werden Anmeldeinformationen für ein SecurityCenter-Administratorkonto benötigt. Wenn Sie über solche Anmeldeinformationen nicht verfügen, erstellen Sie vor dem Ausführen dieses Tasks ein Synchronisierungsadministrator-Konto.

3 **Erstellen Sie in der Systemstruktur einen Container (*Synchronisierungspunkt*) für McAfee SaaS-Daten.**

Synchronisierte Daten von McAfee SaaS-verwalteten Systemen werden in diesen Container verschoben.

4 **Synchronisieren Sie SaaS-Daten aus dem SecurityCenter mit der ePolicy Orchestrator-Datenbank.**

Dabei werden die aktuellen McAfee SaaS-Daten den Überwachungs- und Berichtsfunktionen der Erweiterung sowie der ePolicy Orchestrator-Software zur Verfügung gestellt.

Siehe auch

Installieren der Produkterweiterung auf Seite 14
Erstellen oder Aktualisieren eines Synchronisierungsadministrator-Kontos auf Seite 28
Registrieren eines SecurityCenter-Kontos auf Seite 17
Erstellen eines Synchronisierungspunkts in der Systemstruktur auf Seite 21
Synchronisieren von Daten vom SecurityCenter auf Seite 22

Funktionen, die der ePolicy Orchestrator-Umgebung hinzugefügt wurden

Die Erweiterung ergänzt die ePolicy Orchestrator-Umgebung mit diesen Funktionen oder ruft damit Daten aus einem SecurityCenter-Konto ab und synchronisiert sie mit dem ePolicy Orchestrator-Server.

Tabelle 2-1 Funktionen, die zum Synchronisieren von SaaS-Daten hinzugefügt wurden

Funktion	Informationen
Registrierte Server	Ein Typ eines registrierten Datenbank-Servers ist erforderlich: • **SecurityCenter-Konto**: Für jedes SecurityCenter-Konto, das Sie registrieren möchten, werden Anmeldeinformationen benötigt.
Server-Tasks	Es wird ein vorkonfigurierter, geplanter Abruf-Task hinzugefügt: • **SaaS-Datensynchronisierung**: Ruft Daten aus dem registrierten SecurityCenter-Konto ab und synchronisiert diese mit der ePolicy Orchestrator-Datenbank. Dieser Server-Task ist standardmäßig deaktiviert. Dem Menü **Aktionen** wird eine neue Option hinzugefügt: • **SaaS-Systeme synchronisieren**
Systemstruktur	Fügt auf der Registerkarte **Gruppendetails** im Menü **Aktionen** zwei neue Optionen hinzu: • **Gruppensynchronisierungseinstellungen verwalten**: Damit können Sie einem registrierten SecurityCenter-Konto eine Gruppe zuweisen. (Die Gruppe wird der *Synchronisierungspunkt* des Kontos.) • **Alle SaaS-Synchronisierungspunkte auflisten** – Zeigt an, wann Daten zuletzt für jedes registrierte Konto SecurityCenter-Konto synchronisiert wurden.
Berechtigungssätze	Fügt zwei vorab konfigurierte Benutzerrollen hinzu: • **SaaS-Administrator** – Standardmäßig kann der SaaS-Administrator SaaS-registrierte Server, Server-Tasks und Abfragen erstellen, bearbeiten oder löschen. • **SaaS-Prüfer** – Standardmäßig kann der SaaS-Prüfer registrierte Server und synchronisierte Daten anzeigen und außerdem Abfragen ausführen.

Die Erweiterung beinhaltet zudem Funktionen zur Überwachung der synchronisierten Daten. Diese Funktionen werden an anderer Stelle in diesem Dokument beschrieben.

Siehe auch

Funktionen zur Überwachung von Schutzdiensten auf Seite 30
Konfiguration registrierter Server auf Seite 16
Datensynchronisierung mit SecurityCenter auf Seite 19
Konfiguration von Berechtigungssätzen auf Seite 26

Übersicht über die Funktionskonfiguration

Die Funktionsweise grundlegender Funktionen der Erweiterung kann in der ePolicy Orchestrator-Konsole festgelegt und geändert werden.

Tabelle 2-2 Immer erforderliche Konfigurations-Tasks

Zweck	Vorgehensweise
Registrierte Server	Für jedes SecurityCenter-Konto: • Registrieren Sie das SecurityCenter-Konto beim ePolicy Orchestrator-Server als externen Datenbank-Server. Hierfür werden Anmeldeinformationen für ein SecurityCenter-Konto benötigt. Wenn Sie keine Administratoranmeldeinformationen haben, erstellen Sie vor Anwendung dieser Funktion ein Administratorkonto zur Synchronisierung.
SaaS-Datensynchronisierung, Server-Task	Für jedes registrierte SecurityCenter-Konto: • Konfigurieren Sie einen Synchronisierungspunkt in der Systemstruktur. Dies ist der Speicherort für McAfee SaaS-Daten, die aus dem SecurityCenter abgerufen werden. • Konfigurieren Sie den Server-Task, führen Sie ihn sofort aus, oder legen Sie fest, dass er regelmäßig automatisch ausgeführt wird. Ein Server-Task wird beim Installieren der Erweiterung erstellt. Erstellen Sie bei Bedarf andere Tasks für weitere registrierte SecurityCenter-Konten.

Tabelle 2-3 Gelegentlich erforderliche Konfigurations-Tasks

Zweck	Vorgehensweise
Berechtigungssätze für Benutzerrollen	Für Administratoren, die in Ihrer ePolicy Orchestrator-Umgebung mit der Erweiterung arbeiten: • Gewähren Sie Security-as-a-Service-Benutzerrollen vorhandene Berechtigungssätze, oder erstellen Sie neue Berechtigungssätze, und fügen Sie diese dort hinzu. (Weitere Informationen finden Sie in der Dokumentation zu ePolicy Orchestrator.) • Geben Sie für jede Rolle Berechtigungssätze für den Zugriff (Lese-/Schreibzugriff) an.
Administratorkonto zur Synchronisierung	Für Benutzer, die keine Anmeldeinformationen für ein SecurityCenter-Administratorkonto haben. • Erstellen Sie ein Synchronisierungsadministrator-Konto. Dieses Konto ist zum Konfigurieren von registrierten Servern und Server-Tasks erforderlich. Wenn ein Administratorkonto zur Synchronisierung erforderlich ist, werden im SecurityCenter auf der Seite **Dienstprogramme** auf der Registerkarte **ePO-Server** Links zum Erstellen und Bearbeiten des Kontos angezeigt.

Siehe auch

Installieren der Produkterweiterung auf Seite 14
Registrieren eines SecurityCenter-Kontos auf Seite 17
Erstellen eines Synchronisierungspunkts in der Systemstruktur auf Seite 21
Synchronisieren von Daten vom SecurityCenter auf Seite 22

Installieren der Produkterweiterung

Damit McAfee SaaS-Schutzdienste mithilfe der ePolicy Orchestrator-Software verwaltet werden können, muss zuerst die Security-as-a-Service-Erweiterung heruntergeladen und installiert werden.

> **Bevor Sie beginnen**
>
> Wenn Sie die Erweiterung bereits installiert und deinstalliert haben, müssen einige übrig gebliebene Dateien manuell entfernt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

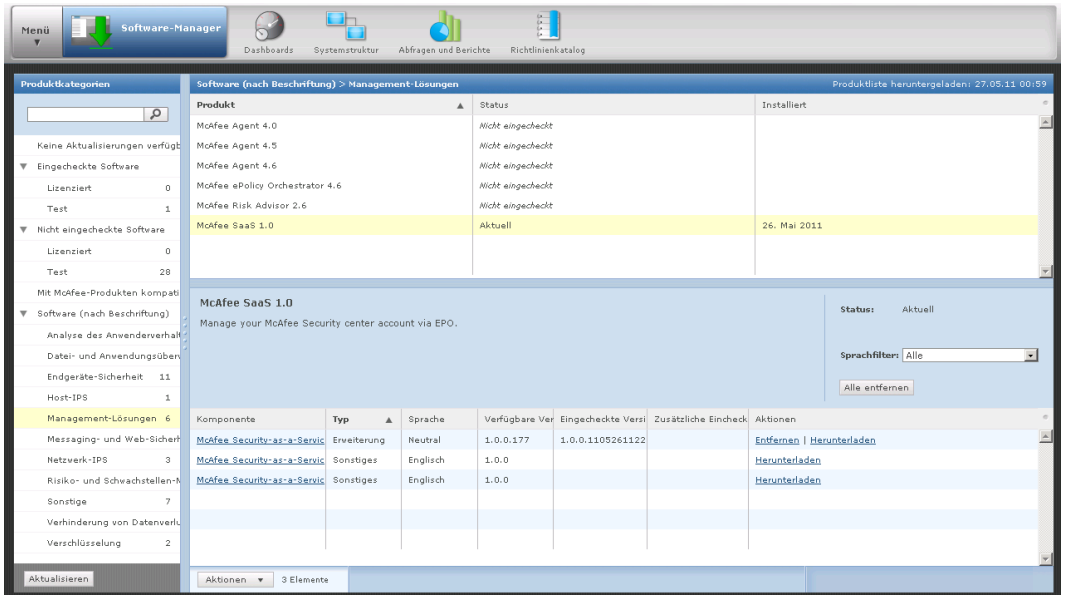
1 Laden Sie die Erweiterung mithilfe einem der folgenden Verfahren herunter:

Über die ePolicy Orchestrator-Konsole

a Klicken Sie auf **Menü** | **Software** | **Software-Manager** | **Erweiterungen**.

b Klicken Sie im Bereich **Produktkategorien** auf **Verwaltungslösungen**.

c Klicken Sie rechts unter **Software** auf **McAfee SaaS <Versionsnummer>**.

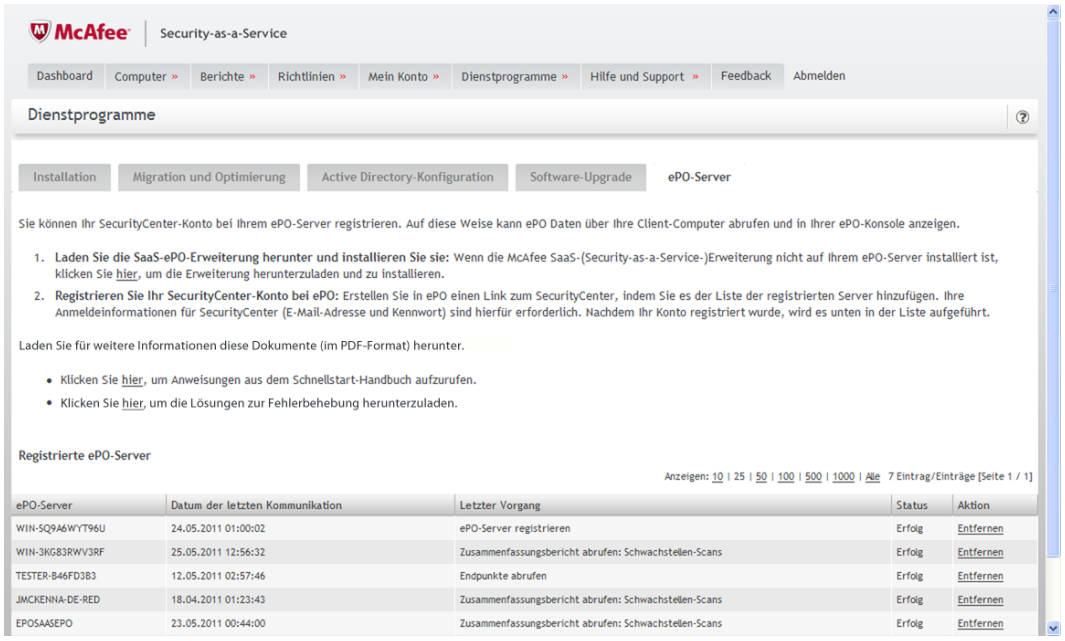


d Suchen Sie im rechten Bereich unter **Komponenten** die Erweiterung, und klicken Sie anschließend auf **Herunterladen**.

e Speichern Sie im Dialogfeld **Datei-Download** die Datei "McAfee Security-as-a-Service.zip" in einen lokalen Ordner, und klicken Sie anschließend auf **OK**.

Über die SecurityCenter-Konsole

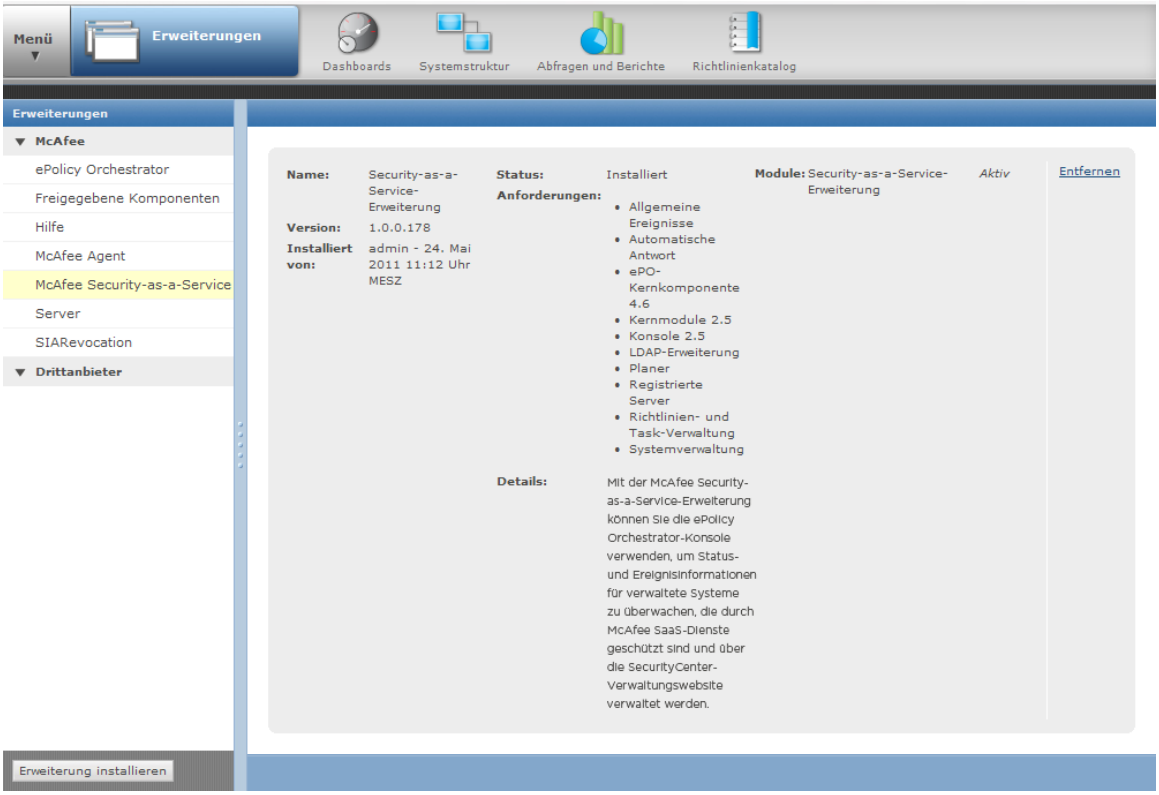
a Klicken Sie auf der Seite **Dienstprogramme** auf die Registerkarte **ePO-Server**.


McAfee
Security-as-a-Service
Dashboard
Computer »
Berichte »
Richtlinien »
Mein Konto »
Dienstprogramme »
Hilfe und Support »
Feedback
Abmelden
Dienstprogramme
Installation
Migration und Optimierung
Active Directory-Konfiguration
Software-Upgrade
ePO-Server
Sie können Ihr SecurityCenter-Konto bei Ihrem ePO-Server registrieren. Auf diese Weise kann ePO Daten über Ihre Client-Computer abrufen und in Ihrer ePO-Konsole anzeigen.
1. Laden Sie die SaaS-ePO-Erweiterung herunter und installieren Sie sie: Wenn die McAfee SaaS-(Security-as-a-Service-)Erweiterung nicht auf Ihrem ePO-Server installiert ist, klicken Sie hier, um die Erweiterung herunterzuladen und zu installieren.
2. Registrieren Sie Ihr SecurityCenter-Konto bei ePO: Erstellen Sie in ePO einen Link zum SecurityCenter, indem Sie es der Liste der registrierten Server hinzufügen. Ihre Anmeldeinformationen für SecurityCenter (E-Mail-Adresse und Kennwort) sind hierfür erforderlich. Nachdem Ihr Konto registriert wurde, wird es unten in der Liste aufgeführt.
Laden Sie für weitere Informationen diese Dokumente (im PDF-Format) herunter.
• Klicken Sie hier, um Anweisungen aus dem Schnellstart-Handbuch aufzurufen.
• Klicken Sie hier, um die Lösungen zur Fehlerbehebung herunterzuladen.
Registrierte ePO-Server
Anzeigen: 10 | 25 | 50 | 100 | 500 | 1000 | Alle 7 Eintrag/Einträge [Seite 1 / 1]
ePO-Server
Datum der letzten Kommunikation
Letzter Vorgang
Status
Aktion
WIN-SQ9A6WYT96U
24.05.2011 01:00:02
ePO-Server registrieren
Erfolg
Entfernen
WIN-3KG83RWV3RF
25.05.2011 12:56:32
Zusammenfassungsbericht abrufen: Schwachstellen-Scans
Erfolg
Entfernen
TESTER-B46FD3B3
12.05.2011 02:57:46
Endpunkte abrufen
Erfolg
Entfernen
JMCKENNA-DE-RED
18.04.2011 01:23:43
Zusammenfassungsbericht abrufen: Schwachstellen-Scans
Erfolg
Entfernen
EPOSAASEPO
23.05.2011 00:44:00
Zusammenfassungsbericht abrufen: Schwachstellen-Scans
Erfolg
Entfernen

b Klicken Sie zum Herunterladen der Erweiterung auf den Link.

c Speichern Sie im Dialogfeld **Datei-Download** die Datei "McAfee Security-as-a-Service.zip" in einen lokalen Ordner, und klicken Sie anschließend auf **OK**.

2 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Software** | **Erweiterungen**, und wählen Sie im Bereich **Erweiterungen McAfee Security-as-a-Service**. Klicken Sie nun im rechten Bereich auf **Erweiterung installieren**.



Siehe auch

Manuelle Löschung von Dateien und Ereignissen auf Seite 45
Manuelles Löschen von Daten auf Seite 45

Konfiguration registrierter Server

Damit Erweiterung und die SecurityCenter-Datenbank miteinander kommunizieren können, muss jedes SecurityCenter-Konto beim ePolicy Orchestrator-Server registriert werden. Dies kann in der ePolicy Orchestrator-Konsole erfolgen.

Für jedes SecurityCenter-Administratorkonto, das Sie registrieren möchten, werden Anmeldeinformationen benötigt.

Nach der Registrierung eines SecurityCenter-Kontos wird derePolicy Orchestrator-Server von SecurityCenter als registrierter ePolicy Orchestrator-Server erkannt. Eine Liste der registrierten ePolicy Orchestrator-Server kann in der SecurityCenter-Konsole auf der Seite **Dienstprogramme** auf der Registerkarte **ePO-Server** eingesehen werden.

Tabelle 2-4 Tasks für registrierte Server

Konsole	Möglichkeiten
ePolicy Orchestrator	• Registrieren eines Kontos • Bearbeiten der Registrierungsinformationen • Zeigen Sie eine Liste der registrierten Konten an. • Löschen registrierter Konten Nach dem Registrieren oder Löschen eines Kontos in der ePolicy Orchestrator-Konsole wird in der SecurityCenter-Konsole auf der Seite **Dashboard** eine Warnung angezeigt.
SecurityCenter	• Sehen Sie Informationen über den ePolicy Orchestrator-Server ein, auf dem Sie das SecurityCenter-Konto registriert haben. • Löschen Sie die Registrierung des ePolicy Orchestrator-Servers. Weitere Informationen finden Sie in der Dokumentation zu McAfee SaaS Endpoint Protection. Diese befindet sich in der SecurityCenter-Konsole auf der Registerkarte **Hilfe und Support**.

Registrieren eines SecurityCenter-Kontos

Registrieren Sie Ihr SecurityCenter-Konto mithilfe der ePolicy Orchestrator-Software, und profitieren Sie von der Erweiterung, um McAfee SaaS-Daten abzurufen und mit der ePolicy Orchestrator-Datenbank zu synchronisieren.

Bevor Sie beginnen

Wenn Sie keine Anmeldeinformationen für ein SecurityCenter-Administratorkonto haben, erstellen Sie ein Administratorkonto zur Synchronisierung.

Beim Registrieren eines Kontos wird in der SecurityCenter-Konsole auf der Seite **Dashboard** eine Warnung angezeigt.

Wenn Sie über mehrere SecurityCenter-Konten verfügen, registrieren Sie jedes separat.

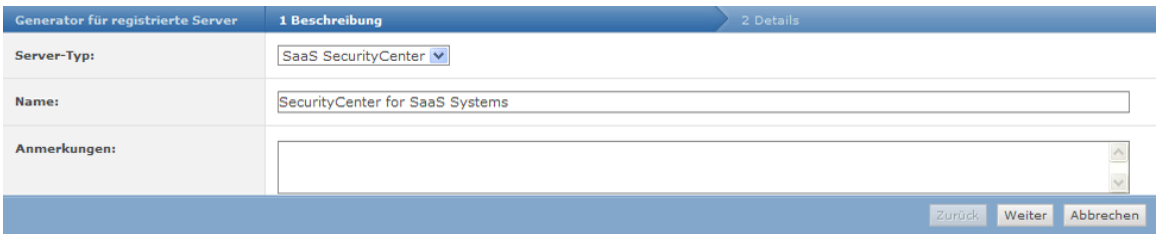
Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Konfiguration** | **Registrierte Server** und danach auf **Neuer Server**.

Der Assistent für den Generator für registrierte Server wird auf der Seite **Beschreibung** geöffnet.

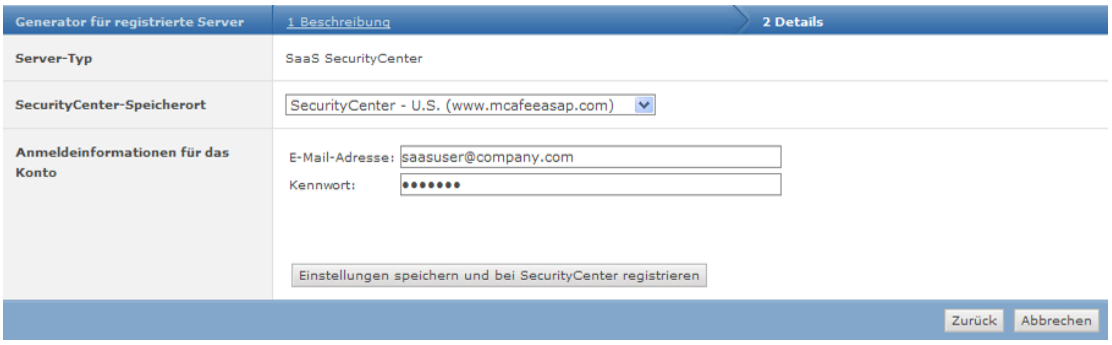
2 Wählen Sie aus der Liste **Server-Typ SaaS SecurityCenter** aus, geben Sie einen Namen und etwaige Hinweise an, und klicken Sie anschließend auf **Weiter**.



3 Wählen Sie aus der Liste **SecurityCenter-Speicherort** das Datenzentrum aus, in dem das Konto gehostet wird.

Das Datenzentrum ist mit dem Domänenteil der URL gekennzeichnet, mit der Sie auf die SecurityCenter-Konsole zugreifen (zum Beispiel www.mcafee.com oder www.*IhrDienstanbieter*.de). Wenn Sie nicht genau wissen, welches Datenzentrum Sie auswählen sollen, sehen Sie sich die URL aus der Begrüßungs-E-Mail an, die Sie nach dem Kauf des Abonnements der McAfee SaaS-Schutzdienste erhalten haben.

4 Geben Sie Ihre Anmeldeinformationen ein, um sich beim SecurityCenter-Konto anzumelden.



Diese haben Sie von Ihrem Dienstanbieter in einer Willkommens-E-Mail erhalten, als Sie ein Abonnement für McAfee SaaS-Schutzdienste erworben haben. Verwenden Sie die Anmeldeinformationen für ein Synchronisierungsadministrator-Konto, wenn Ihnen McAfee oder Ihr Dienstanbieter keine Administratoranmeldeinformationen zugesendet hat.

5 Speichern Sie die Einstellungen mit einer dieser Schaltflächen:

- **Einstellungen speichern und bei SecurityCenter registrieren** – Speichert die Informationen und registriert den Server.
- **Speichern** (untere rechte Ecke) – Speichert die Information ohne Registrierung. Sie können die Registrierung zu einem späteren Zeitpunkt abschließen, ohne die Informationen erneut eingeben zu müssen.

Nach Abschluss der Registrierung wird die E-Mail-Adresse des Kontos im Monitor **McAfee SecurityCenter** im standardmäßigen **Security-as-a-Service-Dashboard** zusammen mit Links zu Seiten in der SecurityCenter-Konsole angezeigt.

Siehe auch

Bereinigen von Bedrohungsereignissen auf Seite 35
Erstellen oder Aktualisieren eines Synchronisierungsadministrator-Kontos auf Seite 28

Anzeigen oder Bearbeiten einer Liste mit registrierten SecurityCenter-Konten

In der ePolicy Orchestrator-Konsole können Sie eine Liste der registrierten SecurityCenter-Konten anzeigen und die Einstellungen nach Bedarf bearbeiten.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Eine Liste aller registrierten Server kann über **Menü** | **Konfiguration** | **Registrierte Server** geöffnet werden.

2 Um die Einstellungen eines Servers zu bearbeiten, wählen Sie in der Liste den gewünschten registrierten Server aus, und klicken Sie anschließend auf **Aktionen** | **Bearbeiten**.

3 Ändern Sie die Einstellungen nach Wunsch, und klicken Sie dann auf **Speichern**.

Löschen eines registrierten SecurityCenter-Kontos

Löschen Sie die Registrierung für ein SecurityCenter-Konto, das nicht mehr verwendet wird. Dies entspricht dem "Aufheben der Registrierung" eines registrierten Servers.

Beim Löschen eines registrierten Servers wird in der SecurityCenter-Konsole auf der Seite **Dashboard** eine Warnung angezeigt.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Konfiguration** | **Registrierte Server**.
2. Wählen Sie den registrierten Server aus der Liste aus, und klicken Sie anschließend auf **Aktionen** | **Löschen**.
3. Löschen Sie in der Systemstruktur den Gruppencontainer, der als Synchronisierungspunkt für das gelöschte Konto fungierte.
   a. Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.
   b. Wählen Sie im Bereich **Systemstruktur** den Gruppencontainer aus.
   c. Klicken Sie auf **Systemstrukturaktionen** | **Gruppe löschen**.
4. Entscheiden Sie, ob Sie die Bedrohungsereignisse des gelöschten Kontos bereinigen möchten.
   - Wenn Sie das SecurityCenter-Konto schließen möchten, können Sie die Bedrohungsereignisse zu Informationszwecken behalten.
   - Soll dasselbe SecurityCenter-Konto zukünftig wieder registriert werden, bereinigen Sie alle Bedrohungsereignisse. Andernfalls werden bei der Synchronisierung von Daten des erneut registrierten Kontos Verlaufsdaten abgerufen, die möglicherweise zu doppelten Ereigniseinträgen führen.

Siehe auch

Bereinigen von Bedrohungsereignissen auf Seite 35

Datensynchronisierung mit SecurityCenter

Bevor Sie McAfee SaaS-Daten in der ePolicy Orchestrator-Konsole anzeigen können, müssen die Daten aus einem registrierten SecurityCenter-Konto abgerufen und mit dem Server und der Datenbank von ePolicy Orchestrator synchronisiert werden.

Nach Installation der Erweiterung wird ein Server-Task zur SaaS-Datensynchronisierung erstellt und so konfiguriert, dass Daten aus einem registrierten SecurityCenter-Konto abgerufen werden.

Die synchronisierten Daten werden in der Systemstruktur und in Monitoren im **Security-as-a-Service**-Dashboard angezeigt. Zudem können Sie mit diesen Daten Abfragen ausführen.

Bei nachfolgenden Aktualisierungen werden die SaaS-Daten aktualisiert und synchronisiert, um die neueren Daten aus dem SecurityCenter-Konto wiederzugeben.

Speicherorte der Daten: Synchronisierungspunkte

Daten zu den mit McAfee SaaS verwalteten Systemen werden in der Systemstruktur in einem bestimmten Container gespeichert. Dies ist ein sogenannter *Synchronisierungspunkt*. Dieser Container muss vor der ersten Ausführung des Server-Tasks erstellt werden. Von diesem Speicherort aus können Sie die durch McAfee SaaS-Dienste geschützten Gruppen und Computer anzeigen.

Wenn Sie über mehrere SecurityCenter-Konten verfügen, erstellen Sie für jedes Konto einen Synchronisierungspunkt und einen Server-Task. Erstellen Sie jeden Synchronisierungspunkt in der obersten Ebene der Systemstruktur. Verschachteln Sie die Gruppen nicht ineinander.

Vollständige und inkrementelle Datensynchronisierung

Wenn von einem Datensynchronisierungs-Task das erste Mal SaaS-Daten aus einem SecurityCenter-Konto abgerufen werden, werden alle entsprechenden Daten der letzten 30 Tage abgerufen. Untere anderem wird anhand des Datenvolumens bestimmt, wie viel Zeit und wie viele Systemressourcen erforderlich sind. Es wird erwartet, dass bei einem anfänglichen Datensynchronisierungs-Task mehr Systemressourcen verwendet werden als bei nachfolgenden Datensynchronisierungs-Tasks für dasselbe SecurityCenter-Konto.

Bei nachfolgenden Datensynchronisierungs-Tasks werden nur die nach der letzten Synchronisierung hinzugefügten oder geänderten Daten abgerufen. Dies führt in der Regel zu einem geringeren Datenvolumen. Daher sind für diese Aktualisierungen normalerweise weniger Ressourcen im Netzwerk, auf dem ePolicy Orchestrator-Server und in der ePolicy Orchestrator-Datenbank (wird möglicherweise auf einem anderen System ausgeführt) erforderlich.

On-Demand- und geplante Datensynchronisierung

Sie können SaaS-Daten bei Bedarf jederzeit synchronisieren, und Sie können die SaaS-Datensynchronisierung so planen, dass sie automatisch in regelmäßigen Intervallen stattfindet.

Die Synchronisierung kann so geplant werden, dass sie in Zeiten mit geringer Netzwerk- und ePolicy Orchestrator-Konsolenaktivität ausgeführt wird. Dies ist möglicherweise eine besonders wichtige Überlegung, wenn Daten das erste Mal aus einem SecurityCenter-Konto abgerufen werden.

Informationen zu den synchronisierten Daten

Sie können die Arten von Daten festlegen, die für die McAfee SaaS-Schutzdienste abgerufen werden sollen, indem Sie Optionen für den Server-Task zur SaaS-Datensynchronisierung auswählen.

Mit dem Server-Task zur SaaS-Datensynchronisierung werden die folgenden Arten von Daten abgerufen:

- Endpunkte (verwaltete Systeme)
- Gruppen, nach denen verwaltete Systeme organisiert sind
- Ereignisse (z. B. Entdeckungen, blockierte Kommunikationsvorgänge, blockierte Websites)
- Schutzstatus
- Zusammenfassende Informationen, die sich auf bestimmte Schutzdienste beziehen, z. B. die Anzahl gescannter E-Mails oder Websites

Nach Abschluss der SaaS-Datensynchronisierung können Sie mit den Überwachungsfunktionen der ePolicy Orchestrator-Software und der Security-as-a-Service-Erweiterung auf die Daten in der ePolicy Orchestrator-Konsole zugreifen.

Siehe auch

Funktionen zur Überwachung von Schutzdiensten auf Seite 30

Erstellen eines Synchronisierungspunkts in der Systemstruktur

Erstellen Sie in der Systemstruktur einen Container zur Speicherung von Daten für McAfee SaaS-Schutzdienste, wenn diese aus dem SecurityCenter-Konto abgerufen und mit der ePolicy Orchestrator-Datenbank synchronisiert werden. Bei diesem Container handelt es sich um einen *Synchronisierungspunkt*.

> **Bevor Sie beginnen**
>
> Registrieren Sie Ihr SecurityCenter-Konto mithilfe der ePolicy Orchestrator-Software. Dazu benötigen Sie die für die Systemstruktur und die Berechtigungssätze für Server-Tasks konfigurierten Berechtigungen. Informationen zur Konfiguration von Berechtigungssätzen finden Sie in der Dokumentation zu ePolicy Orchestrator.

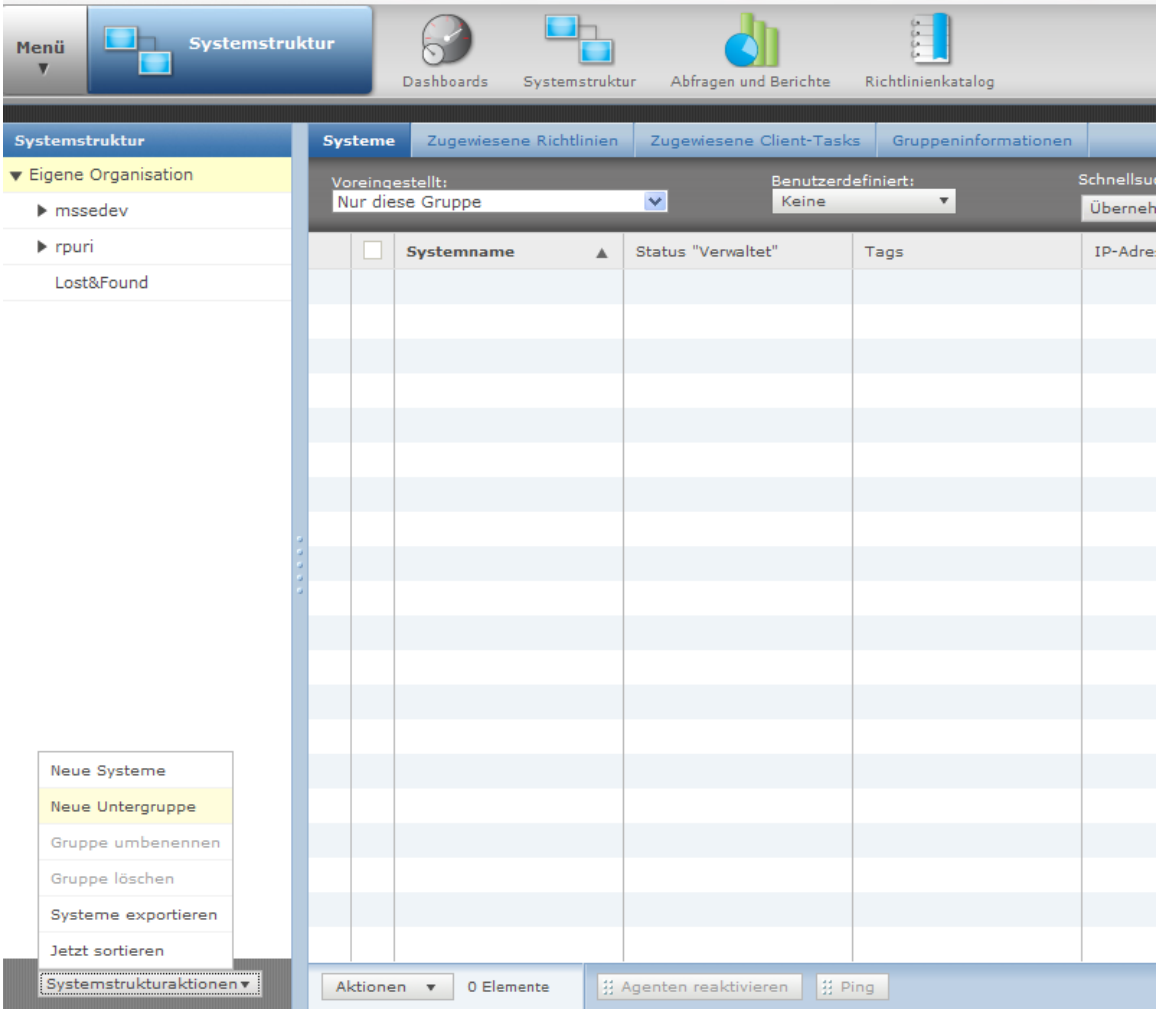
Wenn Sie über mehrere SecurityCenter-Konten verfügen, erstellen Sie für jedes Konto einen separaten Synchronisierungspunkt auf der obersten Ebene der Systemstruktur. Verschachteln Sie nicht einen Synchronisierungscontainer innerhalb eines anderen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Systeme** | **Systemstruktur**.

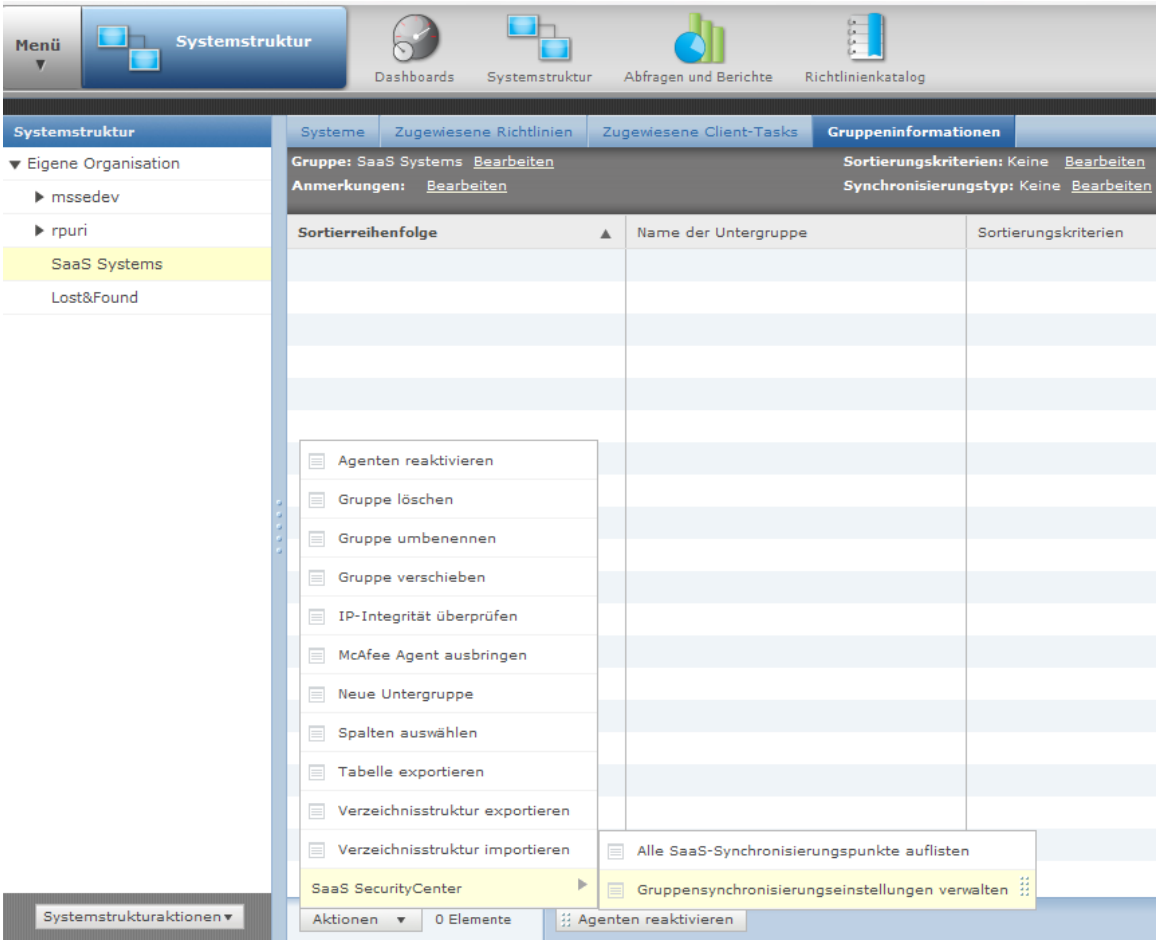
2 Klicken Sie auf **Systemstrukturaktionen** | **Neue Untergruppe**.



3 Geben Sie für die neue Untergruppe einen Namen ein.

4 Wählen Sie in der Systemstruktur die neue Gruppe aus, und klicken Sie anschließend auf die Registerkarte **Gruppeninformationen**.

5 Klicken Sie auf **Aktionen** | **SaaS SecurityCenter** | **Gruppensynchronisierungseinstellungen verwalten**.



6 Wählen Sie ein registriertes SecurityCenter-Konto aus.

7 Speichern Sie die Einstellungen mit einer dieser Schaltflächen:

- **Einstellungen speichern & Jetzt synchronisieren** – Speichert die Synchronisierungseinstellungen und ruft Daten sofort ab.
- **Speichern** (untere rechte Ecke) – Speichert die Einstellungen, ohne Daten abzurufen. Sie können die Synchronisierung zu einem späteren Zeitpunkt durchführen, ohne die Informationen erneut eingeben zu müssen.

Synchronisieren von Daten vom SecurityCenter

Mithilfe eines Server-Tasks können Sie McAfee SaaS-Daten aus einem registrierten SecurityCenter-Konto abrufen und mit der ePolicy Orchestrator-Datenbank synchronisieren. Der Task kann nach Bedarf oder automatisch in regelmäßigen Abständen ausgeführt werden. Zum Beispiel

können Sie den Task so planen, dass die Daten in Ihrem Netzwerk jede Nacht zur gleichen Zeit, also außerhalb der Arbeitszeiten, abgerufen werden.

Bevor Sie beginnen

Registrieren Sie die einzelnen SecurityCenter-Konten mithilfe der ePolicy Orchestrator-Software, und erstellen Sie in der Systemstruktur den zugehörigen Synchronisierungspunkt. Dazu brauchen Sie die für den Berechtigungssatz des Server-Tasks konfigurierten Berechtigungen. Informationen zur Konfiguration von Berechtigungssätzen finden Sie in der Dokumentation zu ePolicy Orchestrator.

Nach Synchronisierung der SaaS-Daten werden die mit McAfee SaaS verwalteten Systeme in der Systemstruktur und die SaaS-Daten in den Monitoren im **Security-as-a-Service**-Dashboard angezeigt.

Wenn Sie einen bestehenden Synchronisierungspunkt löschen, wird der zugehörige Server-Task nicht mehr ausgeführt. Bei erneuter Erstellung des Synchronisierungspunkts müssen Sie den zugehörigen Server-Task erneut konfigurieren oder einen neuen Server-Task erstellen, um für den Synchronisierungspunkt Daten zu synchronisieren. Die erneute Erstellung des Synchronisierungspunkts sorgt nicht dafür, dass der Server-Task, der mit der vorherigen Instanz des Synchronisierungspunkts verknüpft ist, automatisch Daten für die neue Instanz des Synchronisierungspunkts synchronisiert.

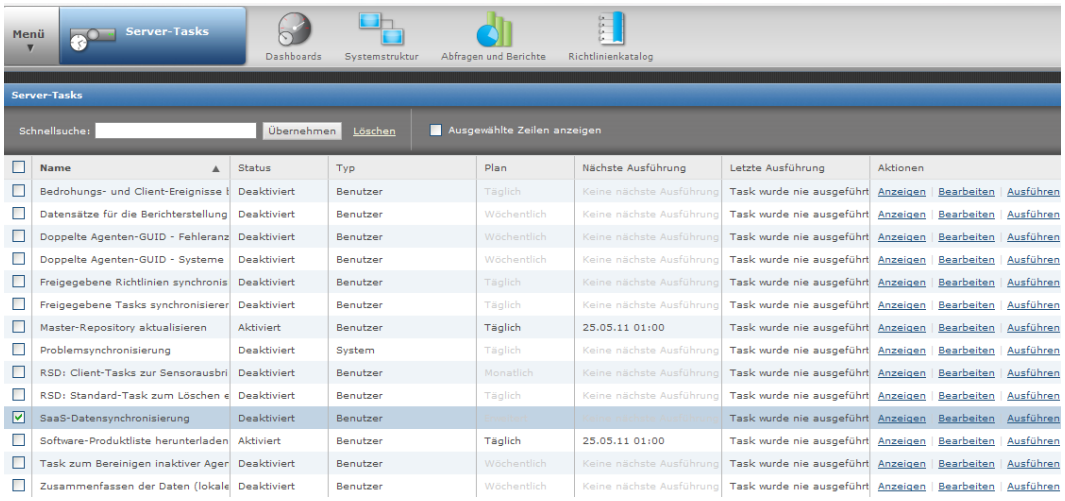
Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Automatisierung** | **Server-Tasks**.

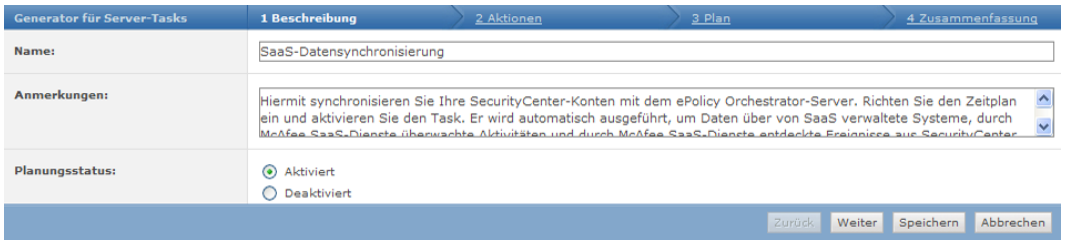
2 Wenn Sie diesen Server-Task zum ersten Mal zur Datensynchronisierung verwenden, müssen Sie ihn wie folgt konfigurieren:

a Suchen Sie in der Liste den Task zur **SaaS-Datensynchronisierung**, und klicken Sie anschließend auf **Bearbeiten**.



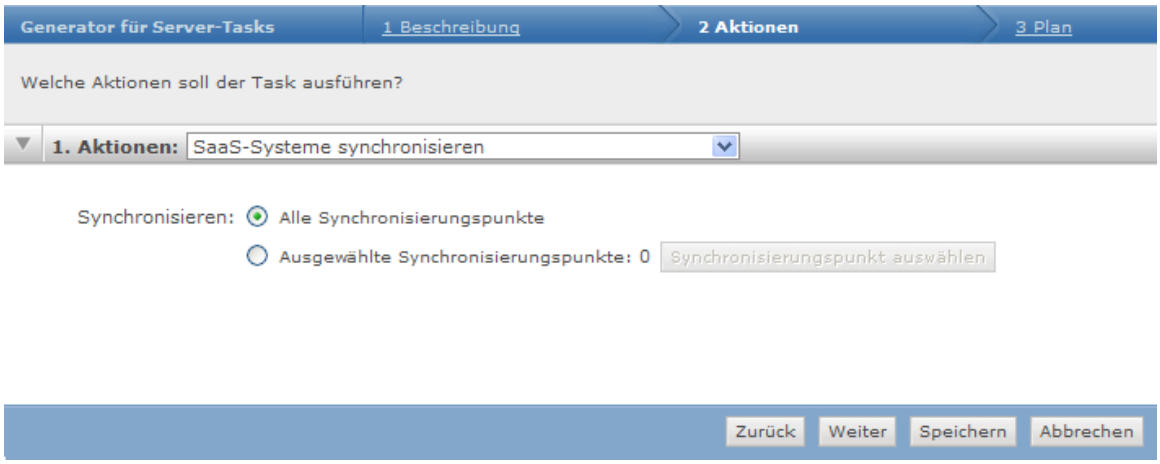
b Geben Sie im Assistenten alle Hinweise ein, die auf der Seite **Beschreibung** angezeigt werden sollen. Wählen Sie dann aus, ob die Zeitplanung aktiviert werden soll, und klicken Sie anschließend auf **Weiter**.

Soll der Server-Task automatisch in regelmäßigen Abständen ausgeführt werden, wählen Sie **Aktiviert** aus, und konfigurieren Sie die Planungsoptionen zu einem späteren Zeitpunkt im Rahmen dieses Tasks. Sie können diese unabhängig von ihrer Aktivierung oder Deaktivierung konfigurieren.



c Prüfen Sie, ob in der Liste **Aktionen** der Eintrag **SaaS-Systeme synchronisieren** ausgewählt ist.

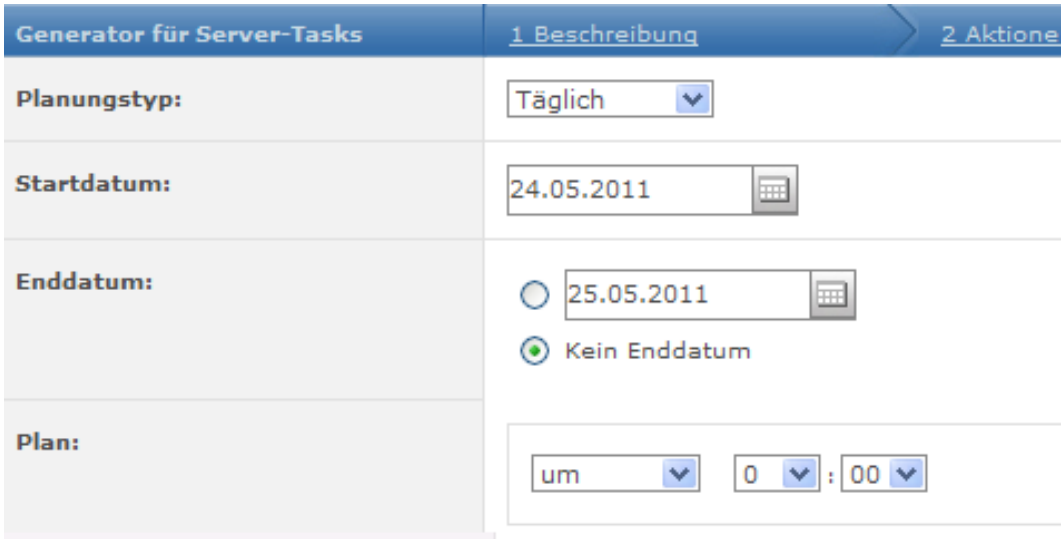
d Wählen Sie für diesen Task die Synchronisierungspunkte aus, und klicken Sie anschließend auf **Weiter**.



Die zu synchronisierenden Arten von Daten sind vorausgewählt.

e Wählen Sie Planungsoptionen aus, und klicken Sie auf **Weiter**.

Diese Auswahl wird ignoriert, es sei denn Sie haben zuvor bei diesem Task die Zeitplanung aktiviert. Sie können die Optionen konfigurieren und speichern und sie dann nach Bedarf aktivieren und deaktivieren.



f Überprüfen Sie die Zusammenfassung, und klicken Sie anschließend auf **Speichern**.

3 Um den Task zu einem beliebigen Zeitpunkt auszuführen, klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**, suchen Sie den Task in der Liste, und klicken Sie danach auf **Ausführen**.

Wenn Sie die Zeitplanung aktiviert haben, wird der Server-Task zu den geplanten Zeiten automatisch ausgeführt.

Siehe auch

Erstellen eines Synchronisierungspunkts in der Systemstruktur auf Seite 21
Erstellen oder Aktualisieren eines Synchronisierungsadministrator-Kontos auf Seite 28

Anzeigen des Status von Synchronisierungspunkten

Überprüfen Sie bei allen Synchronisierungspunkten in der Systemstruktur, ob die McAfee SaaS-Daten aktuell sind.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Systeme** | **Systemstruktur**, und wählen Sie danach eine Gruppe aus.

2 Klicken Sie auf der Registerkarte **Gruppendetails** auf **Aktionen** | **SaaS SecurityCenter** | **Alle SaaS-Synchronisierungspunkte auflisten**, und sehen Sie sich dann die **Letzte Synchronisierungszeit** und die anderen Informationen zu den einzelnen Synchronisierungspunkten an.

Konfiguration von Berechtigungssätzen

Ein Berechtigungssatz ist eine Gruppe von Zugriffsrechten, die einem Benutzerkonto für bestimmte Produktfunktionen gewährt werden. Mit Berechtigungssätzen werden ausschließlich Berechtigungen *gewährt* und niemals entzogen.

Alle Berechtigungen für sämtliche Produkte und Funktionen werden automatisch globalen Administratoren zugewiesen. Anderen Benutzern müssen Berechtigungen manuell zugewiesen werden. Globale Administratoren können vorhandene Berechtigungssätze bei der Erstellung oder Bearbeitung von Benutzerkonten und Berechtigungssätzen zuweisen.

Weitere Informationen zu Berechtigungssätzen finden Sie in der ePolicy Orchestrator-Dokumentation.

Security-as-a-Service-Berechtigungssätze

Die Erweiterung ergänzt die Berechtigungssätze mit einem **Security-as-a-Service**-Bereich. Dieser enthält zwei vorab konfigurierte Benutzerrollen. Die Benutzerrollen bestimmen die Zugriffsrechte auf die Funktionen der Erweiterung. Die globalen Administratoren müssen bestehende Berechtigungssätze für Security-as-a-Service-Benutzerrollen gewähren oder neue Berechtigungssätze erstellen und diese entsprechend hinzufügen.

Tabelle 2-5 Berechtigungen für Security-as-a-Service-Benutzerrollen

Benutzerrollen	Standardberechtigungen
SaaS-Prüfer	Anzeigen registrierter Server und synchronisierter Daten und Ausführen von Abfragen.
SaaS-Administrator	Erstellen, Bearbeiten oder Löschen registrierter Server, Server-Tasks und Abfragen.

Bei Bedarf können globale Administratoren die für diese Rollen festgelegten Berechtigungen ändern oder Berechtigungssätze für neue Rollen erstellen.

Andere erforderliche Berechtigungssätze

ePolicy Orchestrator benötigt Berechtigungen, Zugriff auf andere Funktionen im Hinblick auf die Erweiterung zu gewähren, wie zum Beispiel Abfragen und Dashboards. So brauchen Benutzer zur Verwaltung der SaaS-Datensynchronisierung und der synchronisierten Daten Anzeigeberechtigungen für das Bedrohungsereignisprotokoll, Anzeigeberechtigungen für Systeme, Anzeigeberechtigungen für den Systemstrukturzugriff sowie Anzeige- und Änderungsberechtigungen für den Server-Task zur SaaS-Datensynchronisierung.

Tabelle 2-6 Funktionen und erforderliche Berechtigungen

Funktionen	Erforderliche Berechtigungssätze
Dashboards	Dashboards, Abfragen
Abfragen	Abfragen

Tabelle 2-6 Funktionen und erforderliche Berechtigungen *(Fortsetzung)*

Funktionen	Erforderliche Berechtigungssätze
Server-Tasks	Server-Tasks
Ereignisse bei verwalteten SaaS-Systemen	Systeme, Systemstrukturzugriff, Bedrohungsereignisprotokoll

Konfigurieren von Berechtigungssätzen für Benutzerrollen

Aktualisieren Sie die Berechtigungen für den Lese- und Schreibzugriff, die den Security-as-a-Service-Benutzerrollen zugewiesen sind und für Ihre ePolicy Orchestrator-Umgebung definiert wurden.

Bevor Sie beginnen

Legen Sie die Erweiterungsfunktionen fest, auf die Sie Zugriff gewähren möchten, sowie weitere Berechtigungssätze, die für den Zugriff auf alle Aspekte dieser Funktionen zugewiesen werden müssen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Benutzerverwaltung** | **Berechtigungssätze**.

2 Wählen Sie eine Benutzerrolle aus.

- **SaaS-Administrator**: Kann registrierte Server, Server-Tasks und Abfragen erstellen, bearbeiten und löschen.
- **SaaS-Prüfer**: Kann registrierte Server und synchronisierte Daten anzeigen und Abfragen ausführen.

3 Wählen Sie aus der Liste **Aktionen Bearbeiten**.

4 Wählen Sie für jede Funktion die Berechtigung aus:

- **Keine**
- **Nur Einstellungen anzeigen**
- **Einstellungen anzeigen und ändern**

5 Klicken Sie auf **Speichern**.

Informationen zum Erstellen weiterer Rollen finden Sie in der ePolicy Orchestrator-Dokumentation.

Konfigurieren eines Synchronisierungsadministrator-Kontos

Für Tasks, die eine Kommunikation zwischen dem SecurityCenter-Server und anderen Servern voraussetzen, müssen Anmeldeinformationen für ein SecurityCenter-Administratorkonto angegeben werden.

Wenn Sie noch kein Administratorkonto bei SecurityCenter haben, erstellen Sie vor Durchführung dieser Aufgaben ein Administratorkonto zur Synchronisierung. Dieses Konto stellt die erforderlichen Anmeldeinformationen bereit, mit deren Hilfe Sie speziell für diese Tasks auf das SecurityCenter zugreifen können. (Die Anmeldeinformationen für ein Administratorkonto erhalten Sie in der Regel von McAfee oder dem Anbieter, von dem Sie die McAfee SaaS-Schutzdienste erworben haben.)

Verwenden Sie ein Synchronisierungsadministrator-Konto zu folgenden Zwecken:

- Registrieren Sie das SecurityCenter-Konto mit der ePolicy Orchestrator-Software.
- Ausführen oder Planen einer Datensynchronisierung zwischen dem SecurityCenter-Server und einem Active Directory- oderePolicy Orchestrator-Server.
- Bringen Sie Client-Software auf Systemen in der Active Directory-Domäne unter Verwendung des Push-Installations-Dienstprogramms der SecurityCenter-Konsole aus.

Es kann nur ein Synchronisierungsadministrator-Konto für jeweils ein SecurityCenter-Konto erstellt werden.

Falls ein Synchronisierungsadministrator-Konto erforderlich ist, werden die entsprechenden Links zum Erstellen und Bearbeiten im SecurityCenter auf der Seite **Dienstprogramme** auf der Registerkarte **Active Directory-Konfiguration** oder **ePO-Server** angezeigt.

Erstellen oder Aktualisieren eines Synchronisierungsadministrator-Kontos

Wenn Sie kein SecurityCenter-Administratorkonto haben, müssen Sie ein Synchronisierungsadministrator-Konto erstellen, bevor Sie Tasks ausführen können, bei welchen der SecurityCenter-Server mit anderen Servern kommunizieren muss.

Es kann nur ein Synchronisierungsadministrator-Konto für jeweils ein SecurityCenter-Konto erstellt werden.

Falls Sie über ein SecurityCenter-Administratorkonto verfügen, werden die in diesem Task beschriebenen Links nicht angezeigt. Sie werden nur angezeigt, wenn ein Synchronisierungsadministrator-Konto benötigt wird.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie in der SecurityCenter-Konsole auf die Registerkarte **Dienstprogramme**, und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie auf die Registerkarte **ePO-Server**.
   - Klicken Sie auf die Registerkarte **Active Directory-Konfiguration**.

   Für den Fall, dass Sie ein Administratorkonto erstellen müssen, um einen Task ausführen zu können, wird eine entsprechende Meldung und der Link **Erstellen** angezeigt. Falls bereits ein Administratorkonto besteht, wird eine E-Mail-Adresse für dieses Konto zusammen mit dem Link **Bearbeiten** angezeigt.
2. Klicken Sie auf den passenden Link.
   - **Erstellen** – Geben Sie die E-Mail-Adresse und das Kennwort für das neue Konto ein.
   - **Bearbeiten** – Aktualisieren Sie die E-Mail-Adresse oder das Kennwort für ein bestehendes Konto.
3. Klicken Sie auf **Speichern**.

3 Überwachen und Verwalten der McAfee SaaS-Sicherheit

Die Erweiterungsfunktionen dienen zur Überwachung des Status verwalteter Systeme und Schutzdienste und zur Erkennung von Problemen mithilfe der ePolicy Orchestrator-Konsole.

Inhalt

- *Übersicht über den Überwachungsprozess*
- *Funktionen zur Überwachung von Schutzdiensten*
- *Dashboards und Monitore für Security-as-a-Service*
- *Abfragen und Berichte für Security-as-a-Service*
- *Systeminformationsseite*
- *Bedrohungsereignisprotokoll*
- *Öffnen von SecurityCenter*
- *Kompatibilität mit anderen McAfee-Produkten*

Übersicht über den Überwachungsprozess

Zur Überwachung und Verwaltung der McAfee SaaS-Schutzdienste in einer ePolicy Orchestrator-Umgebung wird ein zweistufiger Ansatz empfohlen.

1 **Zeigen Sie synchronisierte SaaS-Daten in der ePolicy Orchestrator-Konsole an.**

Verwenden Sie die Überwachungsfunktionen der ePolicy Orchestrator-Konsole, um SaaS-Daten zu überprüfen und Probleme mit McAfee SaaS-verwalteten Systemen zu ermitteln.

Tabelle 3-1 Zugriff auf Überwachungsfunktionen

Art der Daten	Wo sie angezeigt werden
Zusammenfassende Informationen zu Status und Aktivität in Tabellen und Diagrammen	**Security-as-a-Service**-Dashboards und -Monitore
Auswählbare Arten von Informationen zum Status der mit McAfee SaaS verwalteten Systeme	**Security-as-a-Service**-Abfragen und -Berichte
McAfee SaaS-Schutzdienste und ihre Eigenschaften	Auf der Seite **Systeminformationen**, auf der Registerkarte **SaaS-Produkte** und Daten im Detailmonitor.
Details zu Entdeckungsereignissen auf McAfee SaaS-verwalteten Systemen	Bedrohungsereignisprotokoll, Security-as-a-Service-Monitore, -Abfragen und -Berichte.

Tabelle 3-1 Zugriff auf Überwachungsfunktionen *(Fortsetzung)*

Art der Daten	Wo sie angezeigt werden
Durch McAfee SaaS-Dienste geschützte Gruppen und Systeme	In der Systemstruktur auf der Registerkarte **Systeme**.
Synchronisierungsstatus für jeden Synchronisierungspunkt	Klicken Sie in der Systemstruktur auf der Registerkarte **Gruppeninformationen** auf **Aktionen** | **SaaS SecurityCenter** | **Alle SaaS-Synchronisierungspunkte auflisten**

2 **Beheben Sie Probleme mit der SecurityCenter-Konsole.**

Mit der SecurityCenter-Konsole können Sie Client-Software auf verwalteten Systemen installieren, Richtlinien konfigurieren und andere Maßnahmen zur Problembehebung ergreifen. Das Standard-Dashboard von **Security-as-a-Service** ermöglicht für jedes registrierte Konto einen einfachen Zugriff über den **McAfee SecurityCenter**-Monitor und beinhaltet direkte Links zur SecurityCenter-Konsole.

Weitere Informationen über die SecurityCenter-Funktionen finden Sie in der Dokumentation zu McAfee SaaS Endpoint Protection. Diese ist in der SecurityCenter-Konsole auf der Seite **Hilfe und Support** erhältlich.

Hinweise zur Überwachung der Sicherheit mit anderen McAfee-Produkten

Prüfen Sie unbedingt, ob Kompatibilitätsprobleme zwischen der Erweiterung und anderer in Ihrer ePolicy Orchestrator-Umgebung ausgeführten McAfee-Software vorliegen, und beheben Sie diese.

Siehe auch

Dashboards und Monitore für Security-as-a-Service auf Seite 31
Abfragen und Berichte für Security-as-a-Service auf Seite 33
Systeminformationsseite auf Seite 34
Bedrohungsereignisprotokoll auf Seite 35
Öffnen von SecurityCenter auf Seite 36
Kompatibilität mit anderen McAfee-Produkten auf Seite 36

Funktionen zur Überwachung von Schutzdiensten

Diese Erweiterung enthält Funktionen zur Anzeige und Überwachung der synchronisierten Daten der McAfee SaaS-Schutzdienste.

Tabelle 3-2 Funktionen für die Überwachung von SaaS-Daten

Funktion in der McAfee ePO-Software	Durch Erweiterung ergänztes Element
Dashboards	Ein vorab konfiguriertes Dashboard: • **Security-as-a-Service** – Zeigt Monitore an, die zu den auf der Seite **Dashboard** in der SecurityCenter-Konsole angezeigten Widgets gehören.
Abfragen	Vorkonfigurierte Abfragen und Optionen zum Erstellen benutzerdefinierter Abfragen: • Neue Gruppe mit gemeinsam verwendeten Abfragen, **Security-as-a-Service**, mit einer Reihe von Abfragen im Zusammenhang mit SaaS-Daten. • Neue Gruppe von Abfrageergebnistypen **Security-as-a-Service** im Abfragen-Generator. Diese Gruppe enthält einen Satz von Abfragezielen im Zusammenhang mit SaaS-Daten.

Tabelle 3-2 Funktionen für die Überwachung von SaaS-Daten *(Fortsetzung)*

Funktion in der McAfee ePO-Software	Durch Erweiterung ergänztes Element
Systemstruktur	Auf der Registerkarte **Gruppeninformationen** gibt es zwei neue **Aktionen**-Menüoptionen: • **SaaS SecurityCenter | Gruppensynchronisierungseinstellungen verwalten** – Damit können Sie einen Gruppencontainer in der Systemstruktur einem registrierten SecurityCenter-Konto zuweisen. (Dies wird der Synchronisierungspunkt für das Konto.) • **SaaS SecurityCenter | Alle SaaS-Synchronisierungspunkte auflisten** – Zeigt an, wann Daten zuletzt für jedes registrierte Konto synchronisiert wurden.
Systeminformationsseite	• Neue Registerkarte **SaaS-Produkte** • Neue Gruppe von Monitoren mit benutzerdefinierbaren Informationen.

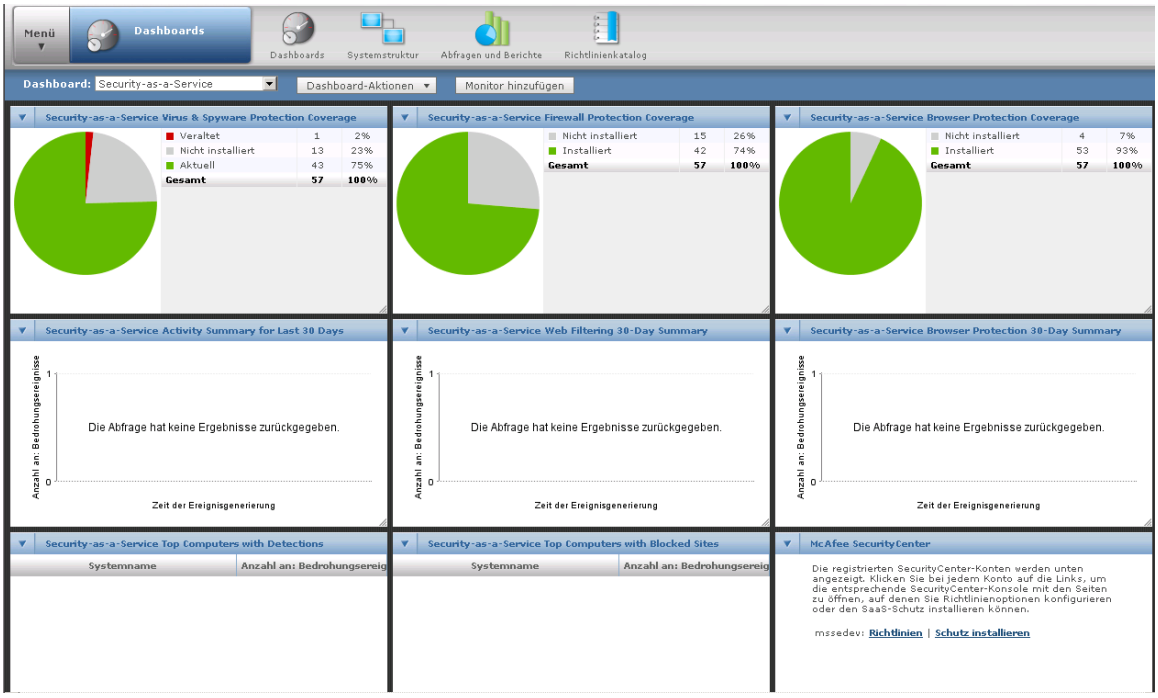
Dashboards und Monitore für Security-as-a-Service

Nachdem die Erweiterung installiert wurde, wird ein vorab konfiguriertes **Security-as-a-Service**-Dashboard erstellt. Darin werden **Security-as-a-Service**-Monitore angezeigt.

Dashboards sind eine Sammlung von Monitoren, die ein wichtiges Tool zum Verwalten Ihrer Umgebung darstellen. Mit den geeigneten Berechtigungen können Sie mehrere Dashboards erstellen und bearbeiten.

Security-as-a-Service-Standard-Dashboard

Die Erweiterung beinhaltet ein Standard-Dashboard mit Monitoren. Diese entsprechen den in SecurityCenter auf der Seite **Dashboard** vorhandenen Widgets. *Widgets* sind kleine interaktive Berichte, die eine Zusammenfassung und Übersicht Ihres Kontos bieten.


Menü
Dashboards
Dashboards
Systemstruktur
Abfragen und Berichte
Richtlinienkatalog
Dashboard: Security-as-a-Service
Dashboard-Aktionen
Monitor hinzufügen
Security-as-a-Service Virus & Spyware Protection Coverage
Veraltet 1 2%
Nicht installiert 13 23%
Aktuell 43 75%
Gesamt 57 100%
Security-as-a-Service Firewall Protection Coverage
Nicht installiert 15 26%
Installiert 42 74%
Gesamt 57 100%
Security-as-a-Service Browser Protection Coverage
Nicht installiert 4 7%
Installiert 53 93%
Gesamt 57 100%
Security-as-a-Service Activity Summary for Last 30 Days
Security-as-a-Service Web Filtering 30-Day Summary
Security-as-a-Service Browser Protection 30-Day Summary
Anzahl an: Bedrohungsereignisse
Die Abfrage hat keine Ergebnisse zurückgegeben.
Zeit der Ereignisgenerierung
Security-as-a-Service Top Computers with Detections
Security-as-a-Service Top Computers with Blocked Sites
Systemname
Anzahl an: Bedrohungsereig
McAfee SecurityCenter
Die registrierten SecurityCenter-Konten werden unten angezeigt. Klicken Sie bei jedem Konto auf die Links, um die entsprechende SecurityCenter-Konsole mit den Seiten zu öffnen, auf denen Sie Richtlinienoptionen konfigurieren oder den SaaS-Schutz installieren können.
mssedev: Richtlinien | Schutz installieren

Wenn Sie sich für mehrere SecurityCenter-Konten registrieren und Daten synchronisieren, werden von den Monitoren Zusammenfassungsdaten zu allen Konten angezeigt.

Für das **Security-as-a-Service**-Dashboard sind folgende SaaS-Datenmonitore verfügbar:

Tabelle 3-3 Security-as-a-Service-Monitore

Monitor	Angezeigte Daten...
McAfee SecurityCenter	Links zu jedem registrierten SecurityCenter-Konto. Klicken Sie auf einen Link, um ein Browser-Fenster zu öffnen und eine Seite in der SecurityCenter-Konsole anzuzeigen.
Abdeckung durch SaaS-Viren- und -Spyware-Schutz	Die Anzahl der Computer in Ihrem Konto, auf denen der Schutz auf dem neuesten Stand, nicht auf dem neuesten Stand und nicht installiert ist. Computer, die auf dem neuesten Stand sind, verfügen über die aktuellen Definitionsdateien zur Entdeckung von Bedrohungen (DAT). Bei Computern, die nicht auf dem neuesten Stand sind, müssen die DAT-Dateien aktualisiert werden. Klicken Sie im Kreisdiagramm des Widgets auf eine Farbe, um eine Liste mit Computern in einer bestimmten Kategorie anzuzeigen.
Abdeckung durch SaaS-Firewall-Schutz	Die Anzahl der Computer in Ihrem Konto, auf denen der Schutz installiert und nicht installiert ist. Klicken Sie im Kreisdiagramm des Widgets auf eine Farbe, um eine Liste mit Computern in einer bestimmten Kategorie anzuzeigen.
Abdeckung durch SaaS-Browser-Schutz	Die Anzahl der Computer in Ihrem Konto, auf denen der Schutz installiert und nicht installiert ist. Klicken Sie im Kreisdiagramm des Widgets auf eine Farbe, um eine Liste mit Computern in einer bestimmten Kategorie anzuzeigen.
SaaS-Computer mit den meisten Entdeckungen	Die Computer mit den meisten entdeckten Bedrohungen innerhalb der letzten sieben Tage. Klicken Sie auf einen Computernamen oder eine Entdeckungsanzahl, um Details anzuzeigen.
SaaS-Computer mit den meisten blockierten Websites	Die Computer mit der höchsten Anzahl an vom Browser-Schutzdienst blockierten Sites in den letzten 7 Tagen. Klicken Sie auf einen Computernamen oder eine Entdeckungsanzahl, um Details anzuzeigen.
SaaS-Aktivitätsübersicht der letzten 30 Tage	Die Anzahl der täglich im vergangenen Monat entdeckten Bedrohungen.
SaaS-Browser-Schutz: 30-Tages-Zusammenfassung	Verlauf der Versuche innerhalb der letzten 30 Tage, blockierte Websites aufzurufen, die mithilfe der Sicherheitsbewertungen von Websites kategorisiert wurden. Zur Anzeige ausführlicher Informationen klicken Sie auf die gewünschte Kategorie.
SaaS-Web-Filterung: 30-Tages-Zusammenfassung	Verlauf der Versuche innerhalb der letzten 30 Tage, Websites aufzurufen, die vom Web-Filterungsdienst blockiert wurden oder vor denen der Benutzer basierend auf Richtlinieneinstellungen für die Inhaltsfilterung gewarnt wird. Zur Anzeige ausführlicher Informationen klicken Sie auf die gewünschte Kategorie.
SaaS-E-Mail-Schutz: 7-Tage-Trend	Die Art und Anzahl der E-Mail-Bedrohungen, die innerhalb der letzten Woche pro Tag vom SaaS-E-Mail-Schutzdienst entdeckt wurden. Klicken Sie auf eine Kategorie, um Details anzuzeigen.
SaaS-E-Mail-Schutz: 7-Tage-Zusammenfassung	Die Gesamtzahl der im Verlauf der letzten Woche an Ihr E-Mail-Konto versendeten Nachrichten, die Art und Anzahl der vom SaaS-E-Mail-Schutzdienst entdeckten Bedrohungen und die Anzahl der Nachrichten ohne Bedrohungen. Klicken Sie auf eine Kategorie, um Details anzuzeigen.
SaaS-Schwachstellen-Scans/ PCI-Zertifizierung	Die Gesamtanzahl der Schwachstellen, die beim letzten Scan entdeckt wurden. Für den Schweregrad gibt es folgende Bewertungen: "Niedrig", "Mittel", "Hoch", "Kritisch" und "Dringend". Klicken Sie auf eine Kategorie, um Details anzuzeigen.

Benutzerdefinierte Dashboards

Sie können benutzerdefinierte Dashboards erstellen und auswählen, welche Monitore und Abfragen angezeigt werden sollen.

Weitere Informationen zum Erstellen und Verwenden von Dashboards finden Sie in der ePolicy Orchestrator-Dokumentation.

Abfragen und Berichte für Security-as-a-Service

Die Erweiterung umfasst die Erstellung von Abfragen und Berichten mithilfe der ePolicy Orchestrator-Software.

Sie können vordefinierte Abfragen verwenden oder anhand von Eigenschaften, die in der ePolicy Orchestrator-Datenbank gespeichert sind, Abfragen erstellen. Weitere Informationen finden Sie in der Dokumentation zu ePolicy Orchestrator.

Die Erweiterung ergänzt die ePolicy Orchestrator-Umgebung mit folgenden Berichtsfunktionen:

- Verschiedene vordefinierte Abfragen, die mit oder ohne Bearbeitung ausgeführt werden können.
- Eine Gruppe von Abfrageergebnistypen, **Security-as-a-Service** im Abfragen-Generator. Die Gruppe enthält eine Reihe von Abfragezielen im Zusammenhang mit SaaS-Daten zur Erstellung benutzerdefinierter Abfragen.

Strukturieren und verwalten Sie benutzerdefinierte Abfragen, um Ihren Anforderungen zu entsprechen. Verwenden Sie sie dann zum Ausführen von Berichten. Sie können Berichte in verschiedene Dateiformate exportieren.

Vordefinierte Abfragen

Die Erweiterung beinhaltet mehrere vorkonfigurierte Abfragen. Sie können diese Abfragen mit ihren Standardeinstellungen verwenden oder sie bearbeiten, um genau die von Ihnen benötigten Informationen zu erhalten.

Die Namen der vordefinierten Abfragen stimmen genau mit den Namen der vordefinierten SaaS-Monitore für das **Security-as-a-Service**-Dashboard überein.

Benutzerdefinierte Abfragen und Berichte

Mit dem Abfragen-Generator lassen sich benutzerdefinierte Abfragen und Berichte erstellen. Anhand der Ergebnistypen, die im Abfragen-Generator ausgewählt wurden, wird ermittelt, welche Art von Daten bei der Abfrage abgerufen werden.

Die Erweiterung ergänzt den Abfragen-Generator mit einer neuen Gruppe von Abfrageergebnistypen, nämlich **Security-as-a-Service**. Diese Gruppe enthält einen Satz von Abfragezielen im Zusammenhang mit SaaS-Daten.

Tabelle 3-4 Security-as-a-Service-Abfrageergebnistypen

Abfrageergebnistyp	Angezeigte Informationen
SaaS-Ereigniseigenschaften	Entdeckungsereignisse
Mit SaaS verwaltete Systeme	Systeme, die über das SecurityCenter verwaltet werden
SaaS-Produkteigenschaften	Eigenschaften für die McAfee SaaS-Produkte, die auf verwalteten Systemen installiert sind
SaaS-Produkte	McAfee SaaS-Produkte in Verwendung
SaaS-Zusammenfassungsberichte	Zusammenfassungsdaten für den SaaS-E-Mail-Schutz und SaaS-Schwachstellen-Scans

Die Erweiterung ergänzt den Abfragen-Generator mit einer Reihe verfügbarer Eigenschaften für jeden Ergebnistyp. Diese können dann in benutzerdefinierten Abfragen verwendet werden.

Weitere Informationen zum Erstellen und Verwenden von Abfragen und Berichten finden Sie in der ePolicy Orchestrator-Dokumentation.

Systeminformationsseite

Die Erweiterung ergänzt die Seite **Systeminformationen** in der ePolicy Orchestrator-Konsole mit Abfragedaten und Produktinformationen.

Sie können auf die Seite **Systeminformationen** zugreifen, indem Sie in der Systemstruktur auf ein beliebiges verwaltetes System klicken.

Monitor- und Abfragedaten

Mit der Ergänzung werden dem anpassbaren Detailmonitor oben rechts auf der Seite **Systeminformationen** Daten hinzugefügt. Um einen Monitor anzuzeigen und auszuwählen, klicken Sie auf **Anpassen**.

Tabelle 3-5 Abfragen, die für den Detailmonitor verfügbar sind

Abfragekategorie	Abfragen
Freigegebene Gruppen – Security-as-a-Service	• Security-as-a-Service-Aktivitätsübersicht für die letzten 30 Tage • Security-as-a-Service-Browser-Schutz: 30-Tages-Zusammenfassung • Security-as-a-Service-Web-Filterung: 30-Tages-Zusammenfassung

Zusammenfassende Informationen sind ausschließlich für die McAfee SaaS-Schutzdienste verfügbar, die für das verwaltete System verwendet werden.

Registerkarte "SaaS-Produkte"

Mit dieser Erweiterung wird die Registerkarte **SaaS-Produkte** erstellt. Auf dieser werden die einzelnen McAfee SaaS-Schutzdienste aufgeführt, die für das verwaltete System verwendet werden.

Auf dieser Registerkarte können Sie die Eigenschaften von jedem Schutzdienst schnell einsehen. Die angezeigten Eigenschaften hängen vom jeweiligen Dienst ab.

Tabelle 3-6 Informationen, die auf der Registerkarte "SaaS-Produkte" angezeigt werden

Eigenschaft	Angezeigte Informationen
Produktbezeichnung	Die Bezeichnung des McAfee SaaS-Schutzdienstes.
Produktversion	Die Produktversionsnummer.
Version des Produktmoduls	Die Produktmodulnummer. Diese wird nur angezeigt, wenn sie für das Produkt gilt und im SecurityCenter-Konto Informationen verfügbar sind.
Produkt-DAT-Version	Die Versionsnummer für die Bedrohungsdefinitionsdatei (DAT), die derzeit verwendet wird. Diese wird nur angezeigt, wenn sie für das Produkt gilt und im SecurityCenter-Konto Informationen verfügbar sind.
Produkt-DAT-Zeitstempel	Das Datum und die Uhrzeit der DAT-Dateierstellung. Dieser Zeitstempel wird nur angezeigt, wenn er für das Produkt gilt und im SecurityCenter-Konto Informationen verfügbar sind.

Bedrohungsereignisprotokoll

Im McAfee-Bedrohungsereignisprotokoll werden Ereignisse angezeigt, die auf den durch McAfee SaaS-Dienste geschützten verwalteten Systemen entdeckt wurden.

Rufen Sie das Bedrohungsereignisprotokoll auf, indem Sie in der ePolicy Orchestrator-Konsole auf **Menü** | **Berichte** | **Bedrohungsereignisprotokoll** klicken. Dort können Sie weitere Informationen über diese Ereignisse und geeignete Lösungsmöglichkeiten einsehen.

- Viren- und Spyware-Entdeckungen
- Vom Firewall-Dienst blockierte eingehende Ereignisse
- Ereignisse zur Web-Filterung

Die zu den Ereignissen angegebenen Datums- und Uhrzeitangaben geben die Ortszeit des ePolicy Orchestrator-Servers an, zu der die Ereignisse aufgetreten sind. Im Gegensatz dazu wird mit der Zeitangabe zu den Ereignissen in den SecurityCenter-Berichten die Ortszeit der verwalteten Systeme angezeigt, in denen das Ereignis aufgetreten ist.

Weitere Informationen zum Bedrohungsereignisprotokoll finden Sie in der ePolicy Orchestrator-Dokumentation.

Zeitpunkt für das Bereinigen von Bedrohungsereignissen

Damit doppelte oder veraltete Daten nicht im Bedrohungsereignisprotokoll angezeigt werden, wird empfohlen, Bedrohungsereignisse in den folgenden Fällen manuell zu bereinigen:

- **Nach dem Löschen eines registrierten SecurityCenter-Kontos**: Wenn Sie ein registriertes Konto aus der Liste der registrierten ePolicy Orchestrator-Server löschen, bereinigen Sie die Bedrohungsereignisse des Kontos. (Soll das Konto nicht erneut registriert werden, können Sie die Bedrohungsereignisse zu Informationszwecken behalten.)
- **Vor der erneuten Installation der Security-as-a-Service-Erweiterung**: Wurde die Software zuvor installiert und wurden SaaS-Daten synchronisiert, bereinigen Sie die zugehörigen Bedrohungsereignisse.

Bereinigen von Bedrohungsereignissen

Wenn Sie die Erweiterung erneut installieren oder ein zuvor registriertes SecurityCenter-Konto erneut registrieren, muss der Inhalt des Bedrohungsereignisprotokolls bereinigt werden. Dadurch wird verhindert, dass veraltete oder doppelte Daten angezeigt werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Bedrohungsereignisprotokoll**.
2. Klicken Sie auf **Aktionen** | **Bereinigen**.
3. Geben Sie im Dialogfeld **Bereinigen** neben **Datensätze bereinigen, die älter sind als:** eine Zahl ein, und wählen Sie eine Zeiteinheit aus.
4. Klicken Sie auf **OK**.

Datensätze, die älter als das angegebene Alter sind, werden dauerhaft gelöscht.

Öffnen von SecurityCenter

Beheben Sie Probleme im Zusammenhang mit McAfee SaaS-Schutzdiensten mit der SecurityCenter-Konsole. Greifen Sie mithilfe des im **Security-as-a-Service**-Dashboard angezeigten Dashboard-Monitors direkt über die ePolicy Orchestrator-Konsole auf die SecurityCenter-Konsole zu.

Bevor Sie beginnen

Registrieren Sie Ihr SecurityCenter-Konto mithilfe der ePolicy Orchestrator-Software.

Weitere Informationen über die SecurityCenter-Funktionen finden Sie in der Dokumentation zu McAfee SaaS Endpoint Protection. Diese ist in der SecurityCenter-Konsole auf der Seite **Hilfe und Support** erhältlich.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1. Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**.
2. Wählen Sie aus der Liste **Dashboards** den Eintrag **Security-as-a-Service** aus.
3. Um ein Web-Browser-Fenster zu öffnen und die SecurityCenter-Konsole aufzurufen, wählen Sie im Monitor **McAfee SecurityCenter** einen der folgenden Links aus:
   - **Richtlinien**: Hiermit wird die Seite **Richtlinie** geöffnet, auf der Sie vorhandene Richtlinien bearbeiten oder neue Richtlinien für verwaltete McAfee SaaS-Systeme erstellen können.
   - **Schutz installieren**: Hiermit wird die Seite **Schutz installieren** geöffnet, auf der Sie die McAfee SaaS-Schutzdienste auf Client-Computern installieren können.

   Wenn Sie über mehrere SecurityCenter-Konten verfügen, werden Links für jedes Konto angezeigt. Sie erkennen das Konto an dem während der Registrierung eingegebenen Namen.

Siehe auch

Registrieren eines SecurityCenter-Kontos auf Seite 17

Kompatibilität mit anderen McAfee-Produkten

Die Erweiterung ist kompatibel mit anderen Produkten von McAfee aus der ePolicy Orchestrator-Umgebung.

Wird die Software mit McAfee® Risk Advisorverwendet, sind jedoch zusätzliche Konfigurationsschritte erforderlich.

Überlegungen zur Verwendung von McAfee Risk Advisor

Scans, die mit McAfee Risk Advisor durchgeführt werden, um verwaltete Systeme zu analysieren und Schwachstellen zu ermitteln, müssen, wenn sie in einer ePolicy Orchestrator-Umgebung mit von McAfee SaaS verwalteten Systemen ausgeführt werden, auf eine bestimmte Weise eingerichtet werden.

McAfee Risk Advisor dient zum Abrufen aktueller Bedrohungsdaten von McAfee® Labs, zur anschließenden Analyse der in der ePolicy Orchestrator-Datenbank gespeicherten Daten und zur Erkennung von Schwachstellen verwalteter Systeme.

Bei mit McAfee SaaS verwalteten Systemen wird nur ein Teil der für die Risikoberechnung relevanten Daten aus dem SecurityCenter-Konto abgerufen und mit der ePolicy Orchestrator-Datenbank synchronisiert. Daher können die Schwachstellen dieser Systeme mit McAfee Risk Advisor nicht genau bewertet werden.

Zwecks einer genaueren Schwachstellenermittlung bei Systemen ohne McAfee SaaS-Dienste wird empfohlen, dieSecurity-as-a-Service-Synchronisierungspunkte aus der Analyse auszuschließen. Verwenden Sie dazu eines der folgenden Verfahren:

- Wählen Sie in der Systemstruktur manuell alle mit McAfee SaaS verwalteten Systeme aus, und deaktivieren Sie für diese die Analyse.
- Erstellen Sie eine ePolicy Orchestrator-Abfrage, um mit McAfee SaaS verwaltete Systeme zu ermitteln, und einen Server-Task, um die Analyse für diese Systeme zu deaktivieren.

Manuelles Ausschließen von verwalteten SaaS-Systemen

Sie können verwaltete McAfee SaaS-Systeme von der Analyse durch McAfee Risk Advisor manuell ausschließen, indem Sie die Systeme in der Systemstruktur auswählen und dann die Analyse für diese deaktivieren.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.

2 Wählen Sie in der Systemstruktur den Synchronisierungspunkt aus, der die McAfee SaaS-verwalteten Systeme enthält.

3 Klicken Sie im rechten Bereich auf die Registerkarte **Systeme**, und wählen Sie anschließend die Systeme aus, die ausgeschlossen werden sollen.

4 Klicken Sie auf **Aktionen** | **Risk Advisor** | **Analysestatus ändern**.

5 Wählen Sie **Deaktivieren** aus, und klicken Sie anschließend auf **OK**.

6 Speichern Sie die Änderung.

   a Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.

   b Klicken Sie rechts auf die Registerkarte **Systeme**, und klicken Sie anschließend auf einen Computernamen.

   c Klicken Sie auf der Seite **Systeminformationen** auf die Registerkarte **Risk Advisor**, und überprüfen Sie dann, ob für **Analysestatus** der Eintrag **Deaktiviert** festgelegt ist.

Ausschließen SaaS-verwalteter Systeme mit einem Server-Task

Um den Prozess zum Ausschließen der mit McAfee SaaS verwalteten Systeme aus der Analyse durch McAfee Risk Advisor zu automatisieren, erstellen Sie eine ePolicy Orchestrator-Abfrage, mit der mit SaaS verwaltete Systeme ermittelt werden, sowie einen Server-Task, um die Analyse für diese Systeme zu deaktivieren.

Die Erweiterung ergänzt die ePolicy Orchestrator-Berichtsfunktion mit dem Verwaltungstyp **Security-as-a-Service**. Mit diesem Verwaltungstyp können Abfragen mit SaaS verwaltete Systeme automatisch ausfindig machen.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

1 Erstellen Sie eine Abfrage, und wählen Sie alle mit McAfee SaaS verwalteten Systeme aus.

   a Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**.

   b Klicken Sie auf die Registerkarte **Abfrage** und anschließend auf **Neu**.

c Legen Sie für die Abfrage Optionen fest.

Registerkarte	Vorgehensweise
Ergebnistyp	**1** Wählen Sie im Bereich **Funktionsgruppe** den Eintrag **Systemverwaltung** aus. **2** Klicken Sie unter **Ergebnistypen** auf **Verwaltete Systeme** und dann auf **Weiter**.
Tabelle	**1** Wählen Sie im Bereich **Ergebnisse anzeigen als** die Option **Tabelle** aus. **2** Wählen Sie rechts **Computereigenschaften** | **Verwaltungstyp** und dann aus der Liste **Sortieren nach** die Option **Verwaltungstyp** aus, und klicken Sie auf **Weiter**.
Spalten	• Fügen Sie im Bereich **Verfügbare Spalten** unter **Computereigenschaften** das Feld **Verwaltungstyp** hinzu. Klicken Sie anschließend auf **Weiter**.
Filter	**1** Fügen Sie im Bereich **Verfügbare Eigenschaften** unter **Computereigenschaften** das Feld **Verwaltungstyp** hinzu. **2** Wählen Sie rechts **Verwaltungstyp** | **Gleich** | **Security as a Service** aus, und klicken Sie auf **Speichern**.

d Geben Sie für die Abfrage einen Namen ein, legen Sie eine neue oder bestehende Abfragegruppe fest, und klicken Sie anschließend auf **Speichern**.

2 Um die Analyse für diese Systeme zu deaktivieren, erstellen Sie einen Server-Task.

a Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**.

b Klicken Sie auf **Neuer Task**.

c Geben Sie für den Task einen Namen ein, wählen Sie für den Planungsstatus **Aktiviert** aus, und klicken Sie anschließend auf **Weiter**.

d Wählen Sie im Menü **Aktionen Abfrage ausführen** aus.

e Klicken Sie im Abfragefeld auf das Browsersymbol, wählen Sie die in Schritt 1 erstellte Abfrage aus der Liste aus, und klicken Sie anschließend auf **OK**.

f Klicken Sie im Feld **Untergeordnete Aktionen** auf das Browsersymbol, wählen Sie aus der Liste **Ereignis(se) oder Anlage(n) deaktivieren oder aktivieren** aus, und klicken Sie anschließend auf **OK**.

g Wählen Sie für **Analysestatus Deaktivieren** aus, und klicken Sie anschließend auf **Weiter**.

h Wählen Sie Planungsoptionen aus, und klicken Sie auf **Weiter**.

i Klicken Sie auf **Speichern**.

3 Führen Sie den Server-Task manuell aus, oder warten Sie, bis dieser entsprechend der Planung ausgeführt wird.

Mit dem Server-Task wird jedes mit SaaS verwaltete System ermittelt und sein **Analysestatus** wird auf **Deaktiviert** festgelegt. Diese Systeme werden bei mit McAfee Risk Advisor durchgeführten Analysen nicht berücksichtigt.

4 Überprüfen Sie die Ergebnisse des Server-Tasks.

   a Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**.

   b Klicken Sie rechts auf die Registerkarte **Systeme**, und klicken Sie anschließend auf einen Computernamen.

   c Klicken Sie auf der Seite **Systeminformationen** auf die Registerkarte **Risk Advisor**, und überprüfen Sie, ob für **Analysestatus** der Eintrag **Deaktiviert** festgelegt ist.

4 Fehlerbehebung

Diese Abschnitte enthalten weitere Informationen zur Installation und Verwendung der Erweiterung.

Inhalt

- *Lösungen zur Fehlerbehebung*
- *Manuelle Löschung von Dateien und Ereignissen*
- *Weitere Informationen*

Lösungen zur Fehlerbehebung

Im Folgenden finden Sie Lösungen häufiger Probleme.

Installieren der Erweiterung

Die Erweiterung wird nicht im Software Download Manager auf dem ePolicy Orchestrator-Server angezeigt.

Laden Sie eine Kopie der Erweiterung aus der SecurityCenter-Konsole herunter. Der entsprechende Link ist auf der Seite **Dienstprogramme** auf der Registerkarte **ePO-Server** angegeben.

Die Erweiterung soll nach einer vorherigen Installation und Deinstallation erneut installiert werden.

Bei der Deinstallation werden nicht alle Elemente entfernt, die mit der Erweiterung verknüpft sind. Bevor Sie die Erweiterung erneut installieren, müssen Sie daher das **Security-as-a-Service**-Dashboard, die **Security-as-a-Service**-Abfragen, den standardmäßigen Server-Task für die SaaS-Datensynchronisierung sowie die Bedrohungsereignisse manuell entfernen.

Herstellen einer Verbindung zum SecurityCenter

In der ePolicy Orchestrator-Konsole kann kein registrierter Server erstellt werden.

Führen Sie mindestens einen der folgenden Vorgänge aus:

- **Überprüfen Sie, ob Sie vom ePolicy Orchestrator-Server aus auf die SecurityCenter-Konsole zugreifen können.** Öffnen Sie auf dem Computer, auf dem der Server ausgeführt wird, ein Browser-Fenster, geben Sie die URL für den Zugriff auf das SecurityCenter ein, und stellen Sie anschließend eine Verbindung her.
- **Überprüfen Sie, ob Ihre Anmeldeinformationen für das SecurityCenter-Konto richtig sind.** Öffnen Sie im gleichen Browser eine neue Registerkarte, oder öffnen Sie ein neues Browser-Fenster. Geben Sie anschließend Ihre Anmeldeinformationen ein, und melden Sie sich an.
- **Überprüfen Sie, ob der ePolicy Orchestrator-Server in der SecurityCenter-Konsole als registrierter Server aufgeführt wird.** Klicken Sie auf der Seite **Dienstprogramme** auf die Registerkarte **ePO-Server**, und überprüfen Sie anschließend die Liste **Registrierte ePolicy Orchestrator-Server**. Wenn Ihr Konto in der Liste aufgeführt ist, können Sie es nicht erneut registrieren. Ist es nicht aufgeführt, wenden Sie sich an den technischen Support.

Registrieren eines Servers

Bei der Registrierung eines SecurityCenter-Kontos wird eine Fehlermeldung angezeigt, die besagt, dass das Konto bereits registriert ist.

Heben Sie die Registrierung des Kontos auf, und registrieren Sie es erneut. Bleibt das Problem weiterhin bestehen, wenden Sie sich an den technischen Support.

Synchronisieren von SaaS-Daten

Nach der Registrierung eines SecurityCenter-Kontos werden keine Daten angezeigt.

Daten werden erst angezeigt, nachdem ein Abruf-Task für den SaaS-Datensynchronisierungsserver erfolgreich ausgeführt wurde.

- **Überprüfen Sie im Server-Task-Protokoll, ob der Task ausgeführt bzw. abgeschlossen wurde.** Wenn die Ausführung des Tasks für eine bestimmte Zeit geplant ist, wurde sie unter Umständen noch nicht ausgeführt. Wenn sie zum ersten Mal ausgeführt wurde, kann die Ausführung sehr lange dauern, da Daten für die vergangenen 30 Tage abgerufen werden.
- **Warten Sie nach Abschluss der Datensynchronisierung drei Minuten, oder aktualisieren Sie die einzelnen Monitore manuell.** Klicken Sie hierfür in jedem Monitor oben links auf das dreieckige Symbol, und wählen Sie anschließend im Menü die Option **Aktualisieren** aus.
- **Überprüfen Sie, ob in der SecurityCenter-Konsole in den Widgets auf der Dashboard-Seite Informationen angezeigt werden.** Wenn Sie Ihr SecurityCenter-Konto erst vor kurzem eingerichtet haben und die Informationen deshalb noch nicht in den Widgets angezeigt werden, können diese mit der ePolicy Orchestrator-Software nicht synchronisiert werden. Werden die Informationen auch nach geraumer Zeit noch nicht in den Widgets angezeigt, gibt es mit Ihrem SecurityCenter-Konto ein Problem. Weitere Informationen finden Sie in der Dokumentation zu McAfee SaaS Endpoint Protection. Diese befindet sich in der SecurityCenter-Konsole auf der Seite **Hilfe und Support**.

Sie erstellen einen Synchronisierungspunkt mithilfe eines bereits registrierten und synchronisierten SecurityCenter-Kontos.

Die Änderung des Synchronisierungspunkts eines registrierten Kontos bedingt nicht, dass auf den Monitoren automatisch Informationen zum neuen Synchronisierungspunkt angezeigt werden. Wird der Synchronisierungspunkt geändert, führen Sie einen der folgenden Vorgänge aus:

- Benennen Sie den bestehenden Synchronisierungspunkt um.
- Löschen Sie vor dem Einrichten des neuen Synchronisierungspunkts die mit McAfee SaaS verwalteten Computer aus dem bestehenden Synchronisierungspunkt.

Für die mit SaaS verwalteten Systeme werden doppelte Daten angezeigt.

Doppelte Daten können in den folgenden Fällen entstehen:

- **Sie haben ein registriertes SecurityCenter-Konto gelöscht, aber den zugehörigen Synchronisierungspunkt nicht manuell gelöscht.** Löschen Sie für das gelöschte Konto den Synchronisierungspunkt, und führen Sie anschließend die SaaS-Datensynchronisierung erneut aus.
- **Sie haben ein registriertes SecurityCenter-Konto gelöscht, aber die Bedrohungsereignisse nicht manuell gelöscht.** Dies hat dazu geführt, dass während der Datensynchronisierung veraltete Bedrohungsereignisse aus der vorherigen Registrierung abgerufen werden. Bereinigen Sie die Bedrohungsereignisse des Kontos, und synchronisieren Sie die Daten anschließend erneut.
- **Sie haben die Erweiterung deinstalliert und erneut installiert, aber die Bedrohungsereignisse nicht manuell gelöscht.** Dies hat dazu geführt, dass während der Datensynchronisierung veraltete Bedrohungsereignisse aus der vorherigen Installation abgerufen werden. Bereinigen Sie die Bedrohungsereignisse des Kontos, und synchronisieren Sie die Daten anschließend erneut.

Sie löschen einen Synchronisierungspunkt und erstellen ihn anschließend erneut.

Wenn Sie einen bestehenden Synchronisierungspunkt löschen, wird der zugehörige Server-Task nicht mehr ausgeführt. Bei erneuter Erstellung des Synchronisierungspunkts müssen Sie den zugehörigen Server-Task konfigurieren oder einen neuen Server-Task erstellen, um für den Synchronisierungspunkt Daten zu synchronisieren. Die erneute Erstellung des Synchronisierungspunkts sorgt nicht dafür, dass der Server-Task, der mit der vorherigen Instanz des Synchronisierungspunkts verknüpft ist, automatisch Daten für die neue Instanz des Synchronisierungspunkts synchronisiert.

Die Daten werden nicht aktualisiert.

Führen Sie einen oder alle der folgenden Schritte aus.

- Überprüfen Sie in der ePolicy Orchestrator-Konsole im Server-Task-Protokoll den Status des Server-Tasks für die SaaS-Datensynchronisierung. Klicken Sie dazu auf **Menü** | **Automatisierung** | **Server-Task-Protokoll**.
- Rufen Sie in der SecurityCenter-Konsole den Synchronisierungsstatus auf. Klicken Sie dazu auf der Seite **Dienstprogramme** auf die Registerkarte **ePO-Server**, und betrachten Sie die Liste **ePolicy Orchestrator(McAfee ePO)-Server**.
- Schlägt der Server-Task zur SaaS-Datensynchronisierung auch weiterhin fehl, wenden Sie sich an den technischen Support. Diesen können Sie über die SecurityCenter-Konsole auf der Registerkarte **Hilfe und Support** unter **Support aufrufen** kontaktieren.

Sie haben einen Synchronisierungspunkt in der Systemstruktur unter einen anderen geschachtelt. Der verschachtelte Synchronisierungspunkt wird jetzt nicht mehr angezeigt.

Wenn Sie für den obersten Synchronisierungspunkt Daten synchronisieren, werden alle Synchronisierungspunkte, die in diesem geschachtelt sind, gelöscht (denn diese Systeme sind nicht im gleichen registrierten Konto vorhanden). Erstellen Sie den gelöschten Synchronisierungspunkt auf der obersten Ebene der Systemstruktur erneut, verknüpfen Sie ihn mit einem Server-Task für die SaaS-Datensynchronisierung, und führen Sie den Server-Task aus, um den Ersatzsynchronisierungspunkt mit durch SaaS verwaltete Systeme auszufüllen.

Keines Ihrer Systeme wird in der Systemstruktur angezeigt.

Innerhalb einer einzelnen Gruppe verwalteter Systeme kann nur eine Instanz eines Systemnamens synchronisiert werden. Wenn Sie innerhalb einer Gruppe mehrere Systeme mit

dem gleichen Namen haben, müssen die Systeme umbenannt und mit eindeutigen Namen versehen werden.

Anzeigen von Daten mit Dashboard-Monitoren

Sie haben Daten synchronisiert, sehen aber in keinem Security-as-a-Service-Dashboard-Monitor Daten.

Nach Abschluss der Synchronisierung werden die Daten in den Dashboard-Monitoren nach drei Minuten automatisch aktualisiert. Um die Daten sofort anzuzeigen, klicken Sie in jedem Monitor oben links auf das dreieckige Symbol, und wählen Sie anschließend im Menü die Option **Aktualisieren** aus.

Durch Klicken auf das Symbol **Aktualisieren** oben rechts in der Konsole werden die Monitore in diesem Fall nicht aktualisiert.

Sie haben Daten synchronisiert, aber die in den Security-as-a-Service-Monitoren angezeigten Daten stimmen nicht mit denen aus den SecurityCenter-Widgets überein.

Die Informationen aus den Monitoren sollten mit den Daten aus den zugehörigen Widgets in der SecurityCenter-Konsole auf der Seite **Dashboard** identisch oder diesen zumindest sehr ähnlich sein. Werden Daten in den Widgets, nicht aber in den Monitoren angezeigt, ist möglicherweise die Konfiguration oder die Synchronisierung der Erweiterung fehlerhaft. Wenden Sie sich an den technischen Support.

Sie haben Daten synchronisiert, sehen in den Monitoren Computer mit den meisten Entdeckungen oder Computer mit den meisten blockierten Websites aber keine Daten.

- In dem vom Monitor festgelegten Zeitraum gab es keine relevanten Entdeckungen.

  Damit Daten in einem Monitor angezeigt werden, muss Ihr SecurityCenter-Konto nicht während der gesamten sieben bzw. 30 Tage aktiv sein. Kontodaten stehen für die Anzahl an Tagen zur Verfügung, an denen das Konto aktiv war.

- Die Datensynchronisierung wurde nicht erfolgreich abgeschlossen oder noch nicht ausgeführt. Überprüfen Sie im Server-Task-Protokoll den Status. Klicken Sie dazu in der ePolicy Orchestrator-Konsole auf **Menü** | **Automatisierung** | **Server-Task-Protokoll**.

- Seit der Synchronisierung sind noch nicht drei Minuten vergangen. Warten Sie, bis die Monitore nach drei Minuten automatisch aktualisiert werden, oder aktualisieren Sie die einzelnen Monitore manuell. Dazu klicken Sie oben links in dem jeweiligen Monitor auf das dreieckige Symbol, und wählen Sie aus dem Menü die Option **Aktualisieren** aus.

Sie haben Daten synchronisiert, sehen aber nicht alle Daten zu Bedrohungsereignissen.

Wenn nach einer SaaS-Datensynchronisierung Bedrohungsereignisse aus dem SecurityCenter fehlen, übersteigt die Datenmenge Ihres Kontos die Menge, die bei einer Task-Ausführung abgerufen werden kann. Planen Sie den Task so, dass er mehrmals täglich ausgeführt wird. So wird gewährleistet, dass alle Bedrohungsereignisse aus dem SecurityCenter abgerufen werden.

Durchführen einer Risikoanalyse

Aus einer McAfee Risk Advisor-Risikoanalyse geht hervor, dass mit McAfee SaaS verwaltete Systeme Risiken ausgesetzt sind.

Nur ein Teil der für die Risikoberechnung relevanten Informationen wird aus dem SecurityCenter-Konto abgerufen und mit der ePolicy Orchestrator-Datenbank synchronisiert. Die Schwachstellen dieser Systeme können deshalb mit der Analyse nicht genau bewertet werden. Genauere Ergebnisse erhalten Sie, wenn Sie mit McAfee SaaS verwaltete Systeme aus der Analyse ausschließen. Dies kann manuell in der Systemstruktur erfolgen, oder Sie erstellen eine Abfrage und einen Server-Task, um diese Systeme automatisch zu ermitteln und auszuschließen.

Siehe auch

Manuelles Ausschließen von verwalteten SaaS-Systemen auf Seite 37
Ausschließen SaaS-verwalteter Systeme mit einem Server-Task auf Seite 37
Manuelles Löschen von Daten auf Seite 45
Bereinigen von Bedrohungsereignissen auf Seite 35

Manuelle Löschung von Dateien und Ereignissen

Beim Entfernen der Erweiterung oder zugehöriger Komponenten aus der ePolicy Orchestrator-Umgebung werden einige Dateien nicht automatisch gelöscht.

In diesen Fällen müssen die Daten manuell gelöscht werden.

- **Nach dem Löschen eines registrierten SecurityCenter-Kontos**
  - Löschen Sie in der Systemstruktur die Containergruppe, in der synchronisierte Gruppen und Systeme gespeichert wurden. (Die Containergruppe in der Systemstruktur ist nicht mehr als Synchronisierungspunkt konfiguriert, enthält aber noch immer die Gruppen und Systeme, die zuvor mit dem gelöschten Konto synchronisiert wurden.)
  - Bereinigen Sie die Bedrohungsereignisse. (Soll das Konto nicht erneut registriert werden, können Sie die Bedrohungsereignisse zu Informationszwecken behalten.)
- **Vor einer Neuinstallation der Erweiterung**
  - Bevor Sie die Erweiterung neu installieren, löschen Sie folgende Elemente manuell:
    - Standard-Task **SaaS-Datensynchronisierung**
    - **Security-as-a-Service**-Dashboard
    - **Security-as-a-Service**-Abfragen
    - Bedrohungsereignisse
  - Löschen Sie diese Elemente nicht. Sie werden bei der ersten SaaS-Datensynchronisierung im Rahmen der neuen Installation automatisch aktualisiert.
    - Registrierte SecurityCenter-Konten
    - Computer und Gruppen, die zuvor mit SecurityCenter synchronisiert wurden
  - Löschen Sie diese Elemente nicht. Sie können in der neuen Installation wiederverwendet oder neu konfiguriert werden.
    - Geplante SaaS-Datensynchronisierungen.

Manuelles Löschen von Daten

Löschen oder bereinigen Sie Elemente, die beim Entfernen der Erweiterung oder ihrer Komponenten aus der ePolicy Orchestrator-Umgebung nicht automatisch gelöscht werden.

Soll die Erweiterung neu installiert werden, müssen nur die Bedrohungsereignisse und die Synchronisierungspunkte gelöscht werden.

Vorgehensweise

Definitionen zu Optionen erhalten Sie, wenn Sie auf der Benutzeroberfläche auf **?** klicken.

- Löschen Sie Elemente bei Bedarf.

Zu löschendes Element	Schritte
Bedrohungsereignisse	1 Klicken Sie auf **Menü** | **Berichterstellung** | **Bedrohungsereignisprotokoll**. 2 Klicken Sie auf **Aktionen** | **Bereinigen**. 3 Geben Sie im Dialogfeld **Bereinigen** neben **Datensätze bereinigen, die älter sind als:** eine Zahl ein, und wählen Sie eine Zeiteinheit aus. 4 Klicken Sie auf **OK**.
Synchronisierungspunkte	1 Klicken Sie auf **Menü** | **Systeme** | **Systemstruktur**. 2 Wählen Sie im Bereich **Systemstruktur** den Synchronisierungspunkt aus. 3 Klicken Sie auf **Systemstrukturaktionen** | **Gruppe löschen**.
Standard-Dashboard	1 Klicken Sie auf **Menü** | **Berichterstellung** | **Dashboards**, und wählen Sie dann das zu löschende Dashboard aus der Dropdown-Liste **Dashboard** aus. 2 Wählen Sie aus der Liste **Dashboards** den Eintrag **Security-as-a-Service**. 3 Klicken Sie auf **Dashboard-Aktionen** | **Löschen**. 4 Klicken Sie auf **OK**.
Standard-Server-Task	1 Klicken Sie auf **Menü** | **Automatisierung** | **Server-Tasks**. 2 Wählen Sie den Server-Task zum **Synchronisieren von SaaS-Daten** aus, und klicken Sie anschließend auf **Aktionen** | **Löschen**. 3 Klicken Sie auf **OK**.
Abfragen	1 Klicken Sie auf **Menü** | **Berichterstellung** | **Abfragen und Berichte**. 2 Wählen Sie die zu löschende Abfrage aus, und klicken Sie anschließend auf **Aktionen** | **Löschen**. 3 Klicken Sie auf **Ja**.

Siehe auch

Installieren der Produkterweiterung auf Seite 14

Weitere Informationen

Greifen Sie auf zusätzliche Dokumentationen zu, um weitere Informationen zur Verwendung der Software zu erhalten.

Vorgehensweise

- Führen Sie einen der folgenden Schritte aus.

Produkt	Zugriff auf Dokumentation
ePolicy Orchestrator-Software	In der ePolicy Orchestrator-Konsole: • Anzeigen der Online-Hilfe: Klicken Sie rechts oben auf einer beliebigen Seite auf **?**. • Herunterladen des Benutzerhandbuchs oder der Versionshinweise: **1** Klicken Sie auf **Menü** | **Software** | **Software-Manager** | **Erweiterungen**. **2** Klicken Sie im Bereich **Produktkategorien** auf **Verwaltungslösungen**. **3** Klicken Sie rechts unter **Software** auf **McAfee ePolicy Orchestrator**. **4** Suchen Sie das Dokument im rechten oberen Bereich der Spalte **Komponente**, und klicken Sie dann in der Spalte **Aktionen** auf **Herunterladen**. **5** Speichern Sie die Dokumentdatei im Dialogfeld **Datei-Download** in einem lokalen Ordner, und klicken Sie dann auf **OK**.
Security-as-a-Service-Erweiterung	In der ePolicy Orchestrator-Konsole: • Anzeigen der Online-Hilfe: Klicken Sie rechts oben auf einer beliebigen Seite mit Inhalten zur Erweiterung auf **?**. • Herunterladen des Benutzerhandbuchs oder der Versionshinweise: **1** Klicken Sie auf **Menü** | **Software** | **Software-Manager** | **Erweiterungen**. **2** Klicken Sie im Bereich **Produktkategorien** auf **Verwaltungslösungen**. **3** Klicken Sie rechts unter **Software** auf **McAfee SaaS <Versionsnummer>**. **4** Suchen Sie das Dokument im rechten oberen Bereich der Spalte **Komponente**, und klicken Sie dann in der Spalte **Aktionen** auf **Herunterladen**. **5** Speichern Sie die Dokumentdatei im Dialogfeld **Datei-Download** in einem lokalen Ordner, und klicken Sie dann auf **OK**.
SecurityCenter, McAfee SaaS Endpoint Protection und McAfee SaaS-Dienste	In der SecurityCenter-Konsole: • Anzeigen der Online-Hilfe: Klicken Sie rechts oben auf einer beliebigen Seite auf **?**. • Anzeigen des Produkthandbuchs oder Installationshandbuchs zu McAfee SaaS Endpoint Protection im PDF-Format: Klicken Sie auf die Registerkarte **Hilfe und Support** und anschließend auf einen Dokument-Link. • Anzeigen einer Kurzanleitung der Erweiterung oder zugehöriger Lösungen zur Fehlerbehebung: Wählen Sie auf

Produkt	Zugriff auf Dokumentation
	der Seite **Dienstprogramme** auf der Registerkarte **ePO-Server** einen der Links aus. • Anzeigen zusätzlicher Dokumentation zu einem bestimmten McAfee SaaS-Dienst: Anweisungen finden Sie im zugehörigen Produkthandbuch im jeweiligen Kapitel. Das zugehörige SaaS-Verwaltungsportal kann in der Regel durch Klicken auf einen Link im zum Dienst gehörigen Widget und dann durch Klicken auf **Hilfe** geöffnet werden.

Index

A

Abfragen für Security-as-a-Service
- Ausschließen von Systemen von der Risikoanalyse 37
- Benutzerdefiniert 33
- Informationen 33
- Löschen 45
- vordefiniert 33

Abfragen-Generator, Security-as-a-Service-Hinzufügungen 33
Abruf von SaaS-Daten, Siehe Datensynchronisierung
Abruf-Tasks, Siehe Server-Tasks für SaaS-Datensynchronisierung
Abrufen von SaaS-Daten, Siehe Datensynchronisierung
Active Directory
- Synchronisierungsadministrator-Konto, erstellen 28
- Synchronisierungsadministrator-Konto, Informationen 27

Administratoren
- Datensynchronisierung, erstellen 28
- Datensynchronisierung, Informationen 27

Anforderungen für Security-as-a-Service-Erweiterung 8
Anzeigen
- Registrierte SecurityCenter-Konten 18
- SaaS-Daten, synchronisiert 29, 30
- SaaS-Datensynchronisierung, Server-Tasks 22
- SaaS-Datensynchronisierung, Status 22
- Synchronisierungspunkte, Status 25

Aufhebung der Registrierung, Server für Security-as-a-Service 19
Ausschluss der mit SaaS verwalteten Systeme aus der Risikoanalyse 36, 37

B

Bearbeiten
- Benutzerrollen für Security-as-a-Service 27
- Berechtigungssätze für Security-as-a-Service 27
- Registrierte SecurityCenter-Konten 18
- SaaS-Datensynchronisierung, Server-Tasks 22
- Synchronisierungsadministrator-Konto 27, 28

Bedrohungsereignisprotokoll
- Bereinigen 35, 45
- Inhalt 35
- Zeitpunkt für Bereinigung 19, 45

Benutzerrollen, Siehe Rollen, Benutzer für Security-as-a-Service
Berechtigungssätze für Security-as-a-Service
- Informationen 26

Berechtigungssätze für Security-as-a-Service *(Fortsetzung)*
- Konfigurieren 27

Bereinigen, Siehe Löschen
Berichte für Security-as-a-Service 33

D

Dashboard für Security-as-a-Service
- Informationen 31
- Standard 31

Dashboards für Security-as-a-Service
- Anpassen 31
- Löschen 45

Datensynchronisierung (Active Directory)
- Synchronisierungsadministrator, erstellen 28
- Synchronisierungsadministrator, Informationen 27

Datensynchronisierung (Security-as-a-Service-Erweiterung)
- Anzeigen des Synchronisierungsstatus 25
- Anzeigen synchronisierter Daten 30
- Definition von SaaS-Daten 20
- Durchführen 22
- Informationen 19
- Planen 22
- Synchronisierungsadministrator, erstellen 28
- Synchronisierungsadministrator, Informationen 27
- Synchronisierungspunkte, Anzeigen des Status 25
- Synchronisierungspunkte, erstellen 21
- Synchronisierungspunkte, Informationen 19

Datenzentrum, auswählen 17
Dokumentation
- Online-Hilfe 46
- Produkt- und Benutzerhandbücher 46
- Produktspezifisch, suchen 6, 46
- Typografische Konventionen und Symbole 5
- Zielgruppe dieses Handbuches 5

E

Einrichtung für die Security-as-a-Service-Erweiterung, Übersicht 8
Ereignisse
- Bedrohungsereignisprotokoll, bereinigen 35
- Bedrohungsereignisprotokoll, Inhalt 35

Erstellen
- Datensynchronisierungspunkte 21

Erstellen *(Fortsetzung)*
Registrierte Server 17
SaaS-Datensynchronisierungszeitplan 22
Synchronisierungsadministrator-Konto 27, 28

G

Geplant, SaaS-Datensynchronisierung 22

H

Handbuch, Informationen 5
Herunterladen, Security-as-a-Service-Erweiterung 14
Hilfe, online 46

I

Installation
Anforderungen 8
Installieren der Security-as-a-Service-Erweiterung 14
Installieren nach früherer Installation 45
Löschen von Daten aus früheren Installationen 45

K

Kompatibilität, Security-as-a-Service und McAfee Risk Advisor 36
Komponenten der Security-as-a-Service-Erweiterung
Einrichtung 8
erforderlich 8
Konfiguration
Benutzerrollen für Security-as-a-Service 27
Berechtigungssätze für Security-as-a-Service 27
McAfee Risk Advisor, Tasks für Risikoanalyse 37
Registrierte Server für Security-as-a-Service-Erweiterung 17
SaaS-Datensynchronisierung 22
Synchronisierungsadministrator-Konto 27, 28
Synchronisierungspunkte 21
Übersicht 13
Konten
Synchronisierungsadministrator, erstellen 28
Synchronisierungsadministrator, Informationen 27
Konventionen und Symbole in diesem Handbuch 5

L

Löschen
Abfragen 45
Dashboards 45
Einträge im Bedrohungsereignisprotokoll 35, 45
Registrierte SecurityCenter-Konten 19
SaaS-verwaltete Systeme von der Risikoanalyse 36
Synchronisierungspunkte 45
Zeitpunkt für manuelle Löschung von Elementen 45

M

McAfee Risk Advisor 36, 37
McAfee SecurityCenter, Siehe SecurityCenter
McAfee SecurityCenter-Monitor 36
McAfee ServicePortal, Zugriff 6
Monitore für Security-as-a-Service
für Systeminformationsseite 34
Informationen 31
McAfee SecurityCenter-Monitor 36
Standard 31

N

Neuinstallation, Anforderungen 45

O

Öffnen, SecurityCenter-Konsole 36
Online-Hilfe 46

P

Protokolle
Bedrohungsereignis 35

R

Registrierte Server für Security-as-a-Service
Anzeigen 18
Bearbeiten 18
Erneutes Registrieren nach früherer Registrierung 45
Informationen 16
Löschen 19
Löschen von Daten aus früheren Registrierungen 45
Registrieren 17
Zugreifen über die McAfee ePO-Konsole 31, 36
Risikoanalyse und Security-as-a-Service 36, 37
Rollen, Benutzer für Security-as-a-Service
Definition 26
Konfigurieren 27
SaaS-Administrator 27
SaaS-Prüfer 27

S

SaaS-Administratorrolle, konfigurieren 27
SaaS-Datensynchronisierung, Siehe Datensynchronisierung
SaaS-Prüferrolle, konfigurieren 27
SaaS-Sicherheit, überwachen
Abfragen, benutzerdefiniert 33
Abfragen, Informationen 33
Abfragen, vordefiniert 33
Bedrohungsereignisprotokoll 35
Berichte 33
Dashboards und Monitore, Informationen 31
Prozessübersicht 29
Systeminformationsseite 34
Überblick über Funktionen 30

SecurityCenter
Aufheben der Registrierung mithilfe der McAfee ePO-Software 19
Definition 7
Dokumentations-Links 46
Herunterladen der Security-as-a-Service-Erweiterung 14
Löschen registrierter ePO-Server 19
Öffnen über die McAfee ePO-Konsole 31, 36
Registrieren mithilfe der McAfee ePO-Software 17
Server-Task zum Ausschließen von Systemen aus der Risikoanalyse 37
Server-Tasks für SaaS-Datensynchronisierung
Anzeigen 22
Ausführen 22
Bearbeiten 22
Definition von Daten 20
Informationen 19
Löschen 45
Planen 22
Überprüfen des Status 19, 25
Server, registriert für Security-as-a-Service
Anzeigen 18
Bearbeiten 18
Informationen 16
Löschen 19
Registrieren 17
ServicePortal, Quellen für Produktdokumentationen 6
Software-Manager
Herunterladen der Dokumentation 46
Herunterladen der Produkterweiterung 14
Synchronisierung, SaaS-Daten, Siehe Datensynchronisierung
Synchronisierungsadministrator
erstellen und aktualisieren 28
Synchronisierungsadministrator *(Fortsetzung)*
Informationen zu 27
Synchronisierungspunkte
Anzeigen des Status 25
Erstellen 21
Informationen 19
Löschen 19, 45
Systemanforderungen 8
Systeminformationsseite 34
Systemstruktur, Synchronisierungspunkte und 21, 25

T

Technischer Support, Produktinformationen suchen 6
Technischer Support, Suchen von Produktinformationen 46

U

Überblick
Einrichtung der Komponenten der Security-as-a-Service-Erweiterung 8
Installation und Einrichtung der Erweiterung 11
SaaS-Funktionen, die der McAfee-Umgebung hinzugefügt wurden 30
Übersicht
Funktionskonfiguration 13
Funktionsweise der Produkterweiterung 7
Prozess zur Überwachung der SaaS-Sicherheit 29
SaaS-Funktionen, die der McAfee-Umgebung hinzugefügt wurden 12
Überwachen der SaaS-Sicherheit, Siehe SaaS-Sicherheit, überwachen